RG-Wall 防火墙命令行手册

(V1.0)

（内部资料，严禁复制）



福建星网锐捷网络有限公司

目 录

1. 导　言

1.1. 本书适用对象

本手册是 RG Wall 防火墙管理员手册中的一本，主要介绍如何通过终端的命令行（Command Line Interface，以下简称 CLI）方式对 RG Wall 防火墙进行配置管理。

本手册适用于负责支持、维护 RG Wall 防火墙的安全管理员，是对 RG Wall 防火墙配置管理的必备手册。

使用本手册的读者，应首先掌握 TCP/IP 协议、IP 地址及子网掩码等基本知识。

1.2. 手册章节组织

本手册按以下的章节编排：

第一章、导言：描述本书适用的读者，手册章节组织、登录命令行界面、命令行概述及相关参考手册等。

第二章、系统配置相关命令：介绍防火墙相关的系统配置，包括：系统时钟、升级许可、导入导出、日志服务器、集中管理、报警邮箱、域名服务器等。

第三章、管理配置相关命令：讲述与防火墙管理相关的配置，包括：管理方式、管理主机、管理员帐号、管理员证书、集中管理等。

第四章、网络配置相关命令：介绍与网络环境相关的配置，包括：网络接口属性、防火墙IP地址、策略路由、ADSL拔号、DHCP配置等。

第五章、VPN配置：讲述VPN的相关配置，包括：VPN基本配置、远程网关、自动IKE隧道、VPN设备、PPTP/L2TP、证书管理等。

第六章、对象定义相关命令：讲述各种对象的定义方法，这些对象可供安全规则使用，包括：地址列表、地址组、服务器地址、NAT地址池、服务列表、服务组、代理服务、时间列表、时间组、连接限制、带宽列表、URL列表等。

第七章、安全策略相关命令：介绍与访问控制相关的配置，包括：安全规则、地址绑定、IDS联动、抗攻击设置等。

第八章、高可用性相关命令：介绍 vrrp 实例和 vrrp 关联的相关配置，包括：vrrp 实例、vrrp 关联、同步配置等。

第九章、用户认证相关命令：介绍与用户认证相关的设置，包括：服务器、用户列表、用户组等。

第十章、系统监控相关命令：描述如何监控系统的运行状态，包括：网络监控、网络接口、隧道监控、日志信息、在线用户、系统 ARP 表、IP 诊断等。

第十一章、其他命令：介绍一些不太常用的命令：如 rcvfile、prompt、dispage 等。

第十二章、命令使用技巧：介绍命令行使用的一些小窍门。

第十三章、命令索引：所有命令的索引，介绍此命令在本手册的哪个页面有详细叙述。

1.3. 登录命令行页面

命令行界面可以使用超级终端通过防火墙上的 CONSOLE 口进入，也可以在远程使用 SSH 客户端进入。

进入命令行界面需要提供用户名和密码，防火墙初始管理员帐号为：admin，其初

始口令为 firewall。

通过超级终端进入 CLI 界面的方法如下：将管理主机的 COM 串口与防火墙的 CONSOLE 口用串口线连接，配置管理主机的超级终端，波特率为 9600 比特。以默认管理员帐号与密码登录，进入命令行界面：

进入 CLI 界面后，出现命令行提示符就可以输入命令，对防火墙进行配置监控了。

在第一次登录成功后，为了安全，管理员应该修改管理员帐号、口令、管理主机、防火墙可管理 IP、管理方式或导入管理员证书等。

1.4. 命令行概述

常用操作及其含义如下表所示：

操作	含义
add	添加
del	删除
set	修改
disp	显示 若指定名称，则显示该名称所代表内容的详细信息；若未指定名称，则显示相应列表的概要信息

所有命令和参数都是大小写敏感的，所有命令其本身都是小写的；命令行的项与项之间必须用空格隔开；当命令行中某项（比如：名称、备注等）包含空格时，必须

用双引号将此字符串包括起来。



（1）如果用户在 180 秒内没有任何操作，CLI 界面会自动退出，返回到登录提示状态。

（2）命令行的所有操作都将记录到系统日志中。

本手册中用到了一些标识（基本参数），其含义如下：

标识	含义	字符长度(个)	可用字符	格式或限制
<id>	序号	1—5	数字	1—65535
<name>	名称	1—20	大、小写英文字母，数字，减号，下划线	第一个字符必须是大、小写英文字母或数字
<comment>	注释	0—255	任意可打印字符，不包括制表符、问号和双引号	无特殊限制
<keyword>	关键字	1—255	任意可打印字符，不包括制表符、问号和双引号	无特殊限制
<password>	口令	6—16	任意可打印字符，不包括制表符、问号和双引号	无特殊限制
<email>	E-Mail 地址	1—64	任意可打印字符，不包括制表符、问号和双引号	Email 标准格式，如 support@ruijie.com.cn
<filename>	文件名	1—254	任意可打印字符，不包括斜线、反斜线、	无特殊限制

标识	含义	字符长度(个)	可用字符	格式或限制
			冒号、星号、问号、双引号、大于号、小于号、管道符、制表符	
<hostname>	主机名	1—254	任意可打印字符，不包括斜线、反斜线、冒号、星号、问号、双引号、大于号、小于号、管道符、制表符	无特殊限制
<number>	数字	1 个以上	正整数	无特殊限制
<percent>	数字	1—3	正整数	0—100
<ip>	单个或多个 IP 地址、IP 地址段	7—31	数字，句号，斜线，冒号	单个 IP 地址（1.1.1.1），IP 地址/子网掩码（1.1.1.0/255.255.255.0），IP 地址段（1.1.1.10:1.1.1.20）
<netmask>	子网掩码	9—15	数字，句号	如 255.255.255.0
<port>	端口	1—11	数字，冒号	单个端口（12345），端口段（1000:7000）

标识	含义	字符长度(个)	可用字符	格式或限制
<mac>	MAC 地址	17	A—F 大小写英文字母，数字，减号，冒号	XX-XX-XX-XX-XX-XX ， 或 XX:XX:XX:XX:XX:XX
<date>	日期	8—10	数字，减号，斜线	yyyy-mm-dd ， 或 yyyy/mm/dd，其中 yyyy 为 2000—2037， mm 为 01—12，dd 为 01—31
<time>	时间	3—17	数字，冒号，减号	时间点为 hh:mm:ss 或 hh:mm，时间段为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm，其中 hh 为 00—23，mm 为 00—59，ss 为 00—59

1.5. 相关参考手册

《星网锐捷 RG Wall 防火墙 WEB 界面手册》，介绍了如何通过 WEB 界面操作管理 RG Wall 防火墙。

《星网锐捷 RG Wall 防火墙快速指南》，介绍了 RG Wall 防火墙的快速安装配置、初始向导的使用等。

《星网锐捷 RG Wall 产品功能使用手册》，描述了 RG Wall 防火墙的复杂功能原理及使用，如 VPN、高可用性、用户认证，并介绍了一些典型案例。

2. 2 系统配置

本章描述与系统本身相关的属性和配置命令，包括：系统时钟、时钟服务器、升级许可、导入导出、报警邮箱、日志服务器、域名服务器等。

2.1. 系统时钟 systime

功能：设置和显示防火墙的系统时钟。

1. 设置系统时钟：

语法：

systime set <date> <time>

参数说明：

<date>	设置日期，格式为 yyyy/mm/dd，yyyy-mm-dd
<time>	设置时间，格式为 hh:mm:ss

不能设置系统时钟早于 2005/09/29 00:00:00!

示例：

firewall>systime set 2005/09/29 13:59:59

2. 显示当前系统时间：

语法：

systime disp

示例：

firewall>systime disp

Clock: 2005/09/29 13:59:59

2.2. 系统启动和运行时间 runtime

功能：

显示系统启动和已运行的时间

语法：

runtime

示例：

firewall>runtime

Started at: 2005/12/28 14:42:56

Already run: 0 day(s) 00:01:28

2.3. 超时退出时间 timeout

1．设置超时退出时间

功能：

设置命令行的超时退出时间，单位是秒。

语法：

timeout { set <number> }

参数说明：

number： 设置命令行无输入时超时时间，number 范围：60~1800 秒，且为整数

示例：

firewall>timeout set 1800

2. 显示超时退出时间

功能：

显示命令行无输入时的超时时间

语法：

timeout disp

示例：

firewall>timeout disp

CLITIMEOUT = 1800 seconds

2.4. 时钟服务器 timesrv

功能：使用网络上的时钟服务器同步防火墙的系统时钟。

1. 设置时钟服务器：

语法：

timesrv set <ip> <number>

参数说明：

ip	设置时钟服务器的 IP 地址
number	设置同步间隔，即每隔多长时间同步一次，有效值为 1 至 65535（分钟）间的正整数

示例：

firewall>timesrv set 192.168.100.160 5

2. 启用时钟服务器：

timesrv on

3. 禁用时钟服务器：

timesrv off

4. 立即与时钟服务器同步：

timesrv sync

5. 清除时钟服务器设置：

timesrv clear

必须先停止使用时钟服务器（timesrv off），才能清除时钟服务器设置。

6. 显示时钟服务器同步设置：

timesrv disp

2.5. 升级许可 sysupdate

功能：对防火墙的软件进行升级。

1. 升级防火墙软件：

语法：

sysupdate <filename>

参数说明：

filename　　升级包文件名称


需要先用命令“rcvfile”上传升级包文件。

示例：

firewall>sysupdate update20050916.pkg

2. 显示防火墙升级历史记录：

sysupdate disp

3. 导入许可证文件：

语法：

license { import <filename.lns> }

参数说明：

filename.lns ：导入的文件名。

4. 显示许可证文件：

license disp

2.6. 系统配置 syscfg

功能：保存系统配置、恢复出厂配置、导入系统配置、导出系统配置。

1. 保存系统配置：

syscfg save

2. 恢复出厂配置：

syscfg reset



执行该命令以后，需要重新启动防火墙，启动成功以后，防火墙配置恢复为出厂配置。

3. 导出系统配置：

语法：

syscfg export <filename> [encrypt { on | off }]

参数说明：

<filename>　　指定导出系统配置的文件名

encrypt　　指定是否对导出的系统配置文件进行加密，可选参数，默认为进行加密

（1）只能在超级终端下可使用该命令，而且所使用的终端必须支持Zmodem 协议（比如 SecureCRT、Windows 自带的"超级终端"）。导出文件所放置的位置必须事先在终端程序中指定，文件名在命令行中指定，使用该命令后文件自动下载到管理主机上相应位置。

（2）导出的系统配置为最近一次保存的系统配置。

示例：

firewall>syscfg export fw.cfg encrypt on

4. 传送配置文件至终端：

语法：

sz <filename>

参数说明：

<filename>　　指定欲传出的系统配置文件名

需要先用命令"syscfg export fw.cfg encrypt on" 创建配置文件，再用本命令导出。

示例：

firewall>sz fw.cfg

5. 导入系统配置：

语法：

syscfg import <filename>

参数说明：

<filename> 指定欲导入的系统配置文件名

需要先用命令“rcvfile”把系统配置文件导入到防火墙上，再执行该命令，然后重新启动防火墙，导入的配置才能生效。

示例：

firewall>syscfg import old.cfg

Please reboot sysinfo.

2.7. 报警邮箱 mngmailbox

功能：设置报警邮箱。当管理员两分钟之内输入错误的登录密码五次时，则发送报警邮件至指定邮箱。

1. 设置报警邮箱和 SMTP 服务器：

语法：

mngmailbox set <email> [smtp <ip> port <port>]

参数说明：

email	设置报警邮箱
smtp	设置发送邮件的 SMTP 服务器，可选参数，默认为空
port	设置 SMTP 服务器的服务端口

示例：

firewall>mngmailbox set support@ruijie.com.cn smtp 192.168.100.1 port 25

2. 清除报警邮箱和 SMTP 服务器设置：

mngmailbox clear

3. 显示报警邮箱和 SMTP 服务器：

mngmailbox disp

2.8. 日志服务器 logsrv

功能：启用日志记录后，默认情况下日志存储在防火墙本地。防火墙也可以将日志发往第三方的日志服务器，此处为设置日志服务器。日志服务器可以与防火墙的任意一个网口连接。

1. 设置日志服务器：

语法：

logsrv set <ip> <port> udp

参数说明：

ip	设置日志服务器的 IP 地址
port	设置日志服务器的端口，UDP 协议的默认端口是 514
udp	设置发送日志使用的协议

示例：

firewall>logsrv set 192.168.100.1 514 udp

2. 清除日志服务器设置：

logsrv clear

3. 显示日志服务器配置：

logsrv disp

2.9. 域名服务器 dns

功能：设置域名服务器和防火墙名称。

1. 设置域名服务器：

语法：

dns set ip <ip> [<ip>]

参数说明：

ip　　设置域名服务器的 IP 地址

示例：

现有两个域名服务器分别为 192.168.1.1 和 192.168.1.2，可以进行如下设置：

firewall>dns set ip 192.168.1.1 192.168.1.2

2. 清除域名服务器和系统主机名设置：

dns clear

3. 显示域名服务器和系统主机名：

dns disp

3. 管理配置

本章描述与管理相关的属性和配置命令，包括：管理方式、管理主机、系统主机名、管理员帐号、口令、证书、集中管理、配置向导等。

3.1. 管理方式 mngmode

功能：设置管理方式。默认情况下，命令行支持“超级终端管理”和“Web 管理”，开启“拨号接入”。在命令行方式下，可以选“SSH 管理（远程管理）”。其中，SSH 管理方式设置后使用网口通信，“超级终端管理”和“拨号接入”通过 CONSOLE 口通信，且不能同时使用。

1. 允许管理员通过 SSH 方式进行管理：

mngmode ssh on

2. 禁止管理员通过 SSH 方式进行管理：

mngmode ssh off



当串口（CONSOLE 口）工作方式为 PPP 时，不能禁用 SSH 管理方式。

3. 显示管理方式：

mngmode disp

3.2. 管理主机 mnghost

功能：设置管理主机。在管理主机上，通过电子钥匙认证或管理员证书认证成功后，再使用管理员帐号认证成功后才能访问防火墙可管理 IP，完成对防火墙的配置管理。

1. 添加管理主机：

语法：

mnghost add <ip> [<comment>]

参数说明：

ip　　　　设置管理主机的 IP 地址

comment　　设置管理主机的注释，可选参数，默认为空

示例：

firewall>mnghost add 192.168.10.1 “This is my host”

2. 删除管理主机：

mnghost del <ip>

3. 显示管理主机：

mnghost disp

3.3. 系统主机名 dns

功能：设置主机的名字。

语法：

dns set sysname <name>

参数说明：

name　　　　　　设置系统主机名

示例：

firewall>dns set sysname firewall

3.4. 管理员帐号 mngacct

功能：设置管理员帐号。在管理主机上，通过电子钥匙认证或管理员证书认证成功后，再使用管理员帐号认证成功后才能访问防火墙可管理 IP，完成对防火墙的配置管理。

1. 添加管理员帐号：

语法：

mngacct add <name> <password> [manager { on | off }] [policyer { on | off }] [auditor { on | off }]

参数说明：

name　　　管理员的名字

password　管理员的密码

manager　　该管理员是否具有修改系统配置的权限，默认为“off”

policyer　　该管理员是否具有修改安全策略（安全规则）的权限，默认为“off”

auditor　　该管理员是否具有审计（查看日志等）权限，默认为“off”

示例：

添加一个管理员，其名称为 adminname，其口令为 pwd@sys123，有修改系统配置和安全规则的权限，没有审计权限。

firewall>mngacct add adminname pwd@sys123 manager on policyer on auditor off

2. 修改管理员帐号：

mngacct set <name> { [password <password>] [manager { on | off }] [policyer { on | off }] [auditor { on | off }] }

3. 删除管理员帐号：

mngacct del <name>

注意 不能删除超级管理员帐号 admin。

4. 允许多个管理员同时管理：

mngacct multi on

5. 禁止多个管理员同时管理：

mngacct multi off

6. 显示管理员帐号信息：

mngacct disp [online [sort { name | time | ip | mode }] | lock]

参数说明：

Online：显示在线管理员

Sort：排序显示

Name：按名称排序

Time：按登录时间排序

Mode：按登录方式排序。有 ssh、web 和串口登录三种

Lock：显示被锁定的用户

7. 为管理员帐号解锁

防火墙在管理员登录错误 5 次以上，即锁定该帐号。此命令允许超级管理员在命

令行模式下，为其他管理员帐号和自己解锁。

mngacct unlock <name>+

3.5. 管理员口令 mngpass

功能：修改当前管理员的密码。

语法：

mngpass

示例：

firewall>mngpass

Current password:

New password:

Retype new password:

Password changed successfully.

3.6. 管理员证书 mngcert

功能：设置管理员证书。在管理主机上，通过电子钥匙认证或管理员证书认证成功后，再使用管理员帐号认证成功后才能访问防火墙可管理 IP，完成对防火墙的配置管理。

1. 添加认证中心证书和防火墙证书：

语法：

mngcert add cacert <filename> syscert <filename> syskey <filename>

参数说明：

cacert　　设置认证中心证书文件名

syscert　　设置防火墙证书文件名

syskey　　设置防火墙密钥文件名

（1）需要先用命令“rcvfile”上传证书文件；（2）仅支持 PEM 格式的证书文件；（3）会覆盖原有的认证中心证书和防火墙证书；（4）会自动删除不再匹配的管理员证书；（5）会重新启动 WEB 服务器，当前的 WEB 连接会被中断，需重新登录到 WEB 界面。（6）当你在 WEB 界面中无意中点了让管理员证书失效的复选框，可执行 mngcert administrator.pem on 命令开启管理员证书。

示例：

firewall>mngcert add cacert cacert123.pem syscert fwcert123.pem syskey fwkey123.pem

2. 添加管理员证书：

语法：

mngcert add <filename>

参数说明：

filename　　管理员证书文件名

需要先用命令“rcvfile”上传证书文件；仅支持 PEM 格式的证书文件。

示例：

firewall>mngcert add admin123.pem

3. 删除管理员证书：

mngcert del <filename>

不能删除已经启用的管理员证书。

4. 启用管理员证书：

mngcert <filename> on

5. 禁用管理员证书：

mngcert <filename> off

6. 显示证书信息：

mngcert disp cacert 显示认证中心证书信息

mngcert disp syscert 显示防火墙证书信息

mngcert disp admincert 显示管理员证书信息

示例：

firewall>mngcert disp admincert

Name: administrator.pem

Status: on

Description: subject= /C=CN/CN=firewallAdmin

3.7. 集中管理 mngglobal

功能：设置集中管理。用于防火墙与集中安全管理系统的无缝联动。

1. 添加集中管理：

语法：

mngglobal add snmpip <ip> [<ip> ...]

参数说明：

snmpip 设置集中管理主机 IP 地址

示例：

firewall>mngglobal add snmpip 192.168.10.100 192.168.10.101

2. 设置集中管理：

语法：

mngglobal set [snmpip <ip>] [cpu <percent>] [mem <percent>] [fs <percent>] [rcomm <string>] [wcomm <string>] [trapc <string>] [status <string>] [principal <string>] [telephone <string>] [comment <string>]

参数说明：

snmpip	设置集中管理主机 IP 地址
cpu	设置 CPU 利用率报警阀值，有效值为 1 至 100
mem	设置内存利用率报警阀值，有效值为 1 至 100
fs	设置文件系统利用率报警阀值，有效值为 1 至 100
rcomm	设置只读团体字符串，1 至 32 个字符
wcomm	设置读写团体字符串，1 至 32 个字符
trapc	设置 Trap 发送字符串, 1 至 32 个字符
status	设置集中管理的状态
principal	设置负责人姓名，1 至 20 个字符
telephone	设置负责人电话，1 至 30 个字符
comment	设置本机备注，1 至 255 个字符

示例：

firewall>mngglobal set snmpip 10.50.10.17 principal support telephone 01062978977 cpu 100 mem 90 fs 80 rcomm “public” wcomm “private” trapc “public” comment “firewall”

3. 清除集中管理所设置的信息：

语法：

mngglobal unset [snmpip] [cpu] [mem] [fs] [rcomm] [wcomm] [trapc] [status] [principal] [telephone] [comment]

参数说明：

snmpip	清除集中管理主机的 IP 地址
cpu	清除集中管理所设置的 CPU 利用率报警阀值，有效值为 1 至 100
mem	清除集中管理所设置的内存利用率报警阀值，有效值为 1 至 100
fs	清除集中管理所设置的文件系统利用率报警阀值，有效值为 1 至 100
rcomm	清除集中管理所设置的只读团体字符串，1 至 32 个字符
wcomm	清除集中管理所设置的读写团体字符串，1 至 32 个字符
trapc	清除集中管理所设置的 Trap 发送字符串, 1 至 32 个字符
status	清除集中管理的状态
principal	清除集中管理所设置的负责人姓名，1 至 20 个字符
telephone	清除集中管理所设置的负责人电话，1 至 30 个字符
comment	清除集中管理所设置的本机备注，1 至 255 个字符

示例：

firewall>mngglobal unset snmpip

4. 删除集中管理主机：

语法：

mngglobal del snmpip <ip> [<ip> ...]

参数说明：

snmpip 指定删除集中管理主机的 IP 地址

示例：

firewall>mngglobal del snmpip 192.168.10.100

5. 启用集中管理：

mngglobal on

指定的集中管理服务器上必须安装并运行集中管理软件（随机光盘内有安装包）。

6. 禁用集中管理：

mngglobal off

7. 显示集中管理设置：

mngglobal disp

8. 是否启用蜂鸣器报警

mngglobal beepalarm on|off

3.8. 初始配置向导 fastsetup

功能：命令行快速配置向导，仅适用于管理员第一次配置防火墙，或者测试防火墙能否正常通信，此命令涉及最基本的配置，安全性很低。因此，管理员应在此基础上对防火墙细化配置，才能保证防火墙拥有正常有效的安全功能。

. 启动初始配置向导：

语法：

fastsetup

参数说明：

无

示例：

firewall>fastsetup



初始配置向导的详细使用，请参见《星网锐捷 RG Wall 防火墙快速指南》

4. 网络配置

本章描述与网络相关的配置命令，包括：网络接口、防火墙 IP 地址、策略路由、ADSL 拨号、DHCP 配置等。

4.1. 网络接口 sysif

功能：设置网络接口属性。

1. 设置网络接口属性：

语法：

sysif set <interface> {[speed { auto | 100full | 100half | 10full | 10half | 1000full | 1000half } [mtu <number>] [ipmac { on | off }] [macpolicy { permit | deny }] [mode { broute | route }] [sroute { on | off }] [log { on | off }] [vlan { <id>+ | trunk | off }] [anti { on | off }] [nonip { permit | deny }] [idsblock { on | off }] }

参数说明：

interface	指定欲设置的网络接口
speed	可选项，各属性值含义为：auto：自协商，100full：百兆全双工，100half：百兆半双工，10full：十兆全双工，10half：十兆半双工，1000full：千兆全双工，1000half：千兆半双工
mtu	设置最大传输单位，有效值为 256 至 1500（字节）
ipmac	设置是否启用 IP/MAC 地址绑定检查
macpolicy	设置 IP/MAC 地址绑定检查的策略，设置为 permit 时，允许未

	绑定的 IP/MAC 地址，设置为 deny 时，禁止未绑定的 IP/MAC 地址。
	注意 仅在启用了 IP/MAC 地址检查后有效
mode	设置网络接口的工作模式，route 为路由模式，broute 为混合模式
	注意 若使用负载均衡模式的集群，则网络接口的工作模式不能为混合模式
sroute	设置网络接口是否启用源路由功能
log	设置网络接口是否记录丢弃的数据包
vlan	设置网络接口的 VLAN 属性，若设置了 ID，则可接收指定 ID 的 VLAN 数据包，若设置为 trunk，则可接收所有 VLAN 数据包，若设置为 off，则不接收 VLAN 数据包
	注意 仅在启用了 vlan 路由（sysif set vlanroute on）后有效
anti	设置网络接口是否启用抗攻击
nonip	设置网络接口是否允许非 IP 协议数据包通过
	注意 此设置仅在网络接口的工作模式为混合模式时有效。当网络接口的工作模式为路由模式时，不允许非 IP 协议数据包通过
idsblock	设置网络接口是否启用 IDS 联动阻断

示例：

假设网络环境需要网络接口 FE1 工作在全双工模式下、打开 ipmac 绑定、启用源

路由、记录日志、设置为路由模式、启用 vlan、允许非 IP 包通过、启用 IDS 阻断。可用以下命令进行设置：

```
firewall>sysif set fe1 mtu 1500
firewall>sysif set fe1 ipmac on
firewall>sysif set fe1 macpolicy permit
firewall>sysif set fe1 mode route
firewall>sysif set fe1 sroute on
firewall>sysif set fe1 log on
firewall>sysif set fe1 vlan 100 200 300
firewall>sysif set fe1 anti on
firewall>sysif set fe1 nonip permit
firewall>sysif set fe1 idsblock on
```

2. 设置 VLAN 路由：

语法：

sysif set vlanroute {on |off}

参数说明：

on	启用 vlan 路由
off	禁用 vlan 路由

3. 显示所有网络接口：

sysif disp	显示所有启动网络接口的属性
sysif disp <interface>	显示指定网络接口属性

4.2. 接口 IP 地址 sysip

功能：设置防火墙 IP 地址。防火墙一般提供 4 个网口（FE1～FE4），百兆扩展模块网口为 S1F1、S1F2、S2F1、S2F2，千兆网口编号为 GE1、GE2、GE3 等。此处以百兆 4 个网口设置 IP 地址为例。

当网口设置为混合模式时，还将生成一个虚网口设备 br，br 使用的 IP 地址为绑定在 br 上的物理设备的 IP 地址。

1. 添加防火墙 IP 地址（其它网络接口）：

语法：

sysip add <interface> <ip> <netmask> [admin { on [ping { on | off }] [traceroute { on | off }] | off]}

参数说明：

interface	设置添加防火墙 IP 地址的网络接口
ip	设置 IP 地址
netmask	设置子网掩码
admin	设置是否可通过此 IP 地址管理防火墙，可选参数，默认为不可管理
ping	设置此 IP 地址是否允许管理主机 ping，可选参数，默认为不允许
traceroute	设置此 IP 地址是否允许管理主机 traceroute，可选参数，默认为不允许

注意：欲添加的 IP 地址不能与其它网络接口上的 IP 地址或地址池在同一子网。

示例：

firewall>sysip add fe1 192.168.100.1 255.255.255.0 admin on ping on traceroute on

2. 删除防火墙 IP 地址：

语法：

sysip del <ip>

参数说明：

ip　　　　指定欲删除的防火墙 IP 地址

注意：不能删除被安全规则引用的防火墙 IP 地址，也不能删除被 HA 基本配置中设置的防火墙 IP 地址。

示例：

firewall>sysip del 192.168.100.1

3. 显示防火墙 IP 地址：

sysip disp

4.3. 策略路由 route

功能：设置静态路由。包括源 IP 路由、目的 IP 路由和路由均衡负载的设置。

1. 添加源路由：

语法：

route add sroute <sip> <dip> <nexthop>

参数说明：

sip　　　　设置源 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、“any”

dip　　设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、“any”

nexthop　　设置下一跳的 IP 地址

注意 最多只能添加 1024 条源路由

示例：

添加一条源路由：从源 IP 192.168.10.100 到网络 192.168.11.0/255.255.255.0 的所有数据包都从网关 10.50.10.200 转发，可进行如下设置：

firewall>route add sroute 192.168.10.100 192.168.11.0/255.255.255.0 10.50.10.200

提示：输入示例中命令之前，必须在相应的网络接口设置允许“按源 IP 路由”（请查看 sysif 命令）。

2. 删除源路由：

语法：

route del sroute <sip> <dip>

参数说明：

sip　　指定欲删除的源路由的源 IP 地址

dip　　指定欲删除的源路由的目的 IP 地址

示例：

firewall>route del sroute 192.168.10.100 192.168.11.100

3. 添加目的路由：

语法：

route add droute <dip> <nexthop> | <vpndev_name>

参数说明：

dip　　设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、“any”

nexthop　　设置下一跳的 IP 地址

vpndev_name　　选择走 vpn 设备

示例：

添加一条目的路由：从其它网络到网络 192.168.11.0/255.255.255.0 的所有数据包都从网关 192.168.12.1 转发，可进行如下设置：

firewall>route add droute 192.168.11.0/255.255.255.0 192.168.12.1

说明：当输入的目的地址为 0.0.0.0/0.0.0.0 时，添加的即为默认网关。

4. 删除目的路由：

语法：

route del droute <dip>

参数说明：

dip　　指定欲删除的目的路由的目的 IP 地址

示例：

firewall>route del droute 192.168.11.0/255.255.255.0

5. 添加路由均衡负载：

语法：

route add mroute <dip> <nexthop> <weight> <nexthop> <weight> [<nexthop> <weight>]

参数说明：

dip　　设置目的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、“any”

nexthop 设置下一跳的 IP 地址

weight 设置下一跳的权值，weight 在 1－100 之间取值

示例：

添加一条负载均衡路由：到网络 192.168.11.100 的所有数据包都从网关 10.50.10.200 和网关 10.50.11.200 转发，可进行如下设置：

firewall>route add mroute 192.168.11.100 10.50.10.200 20 10.50.11.200 80

6. 删除负载均衡路由：

route del mroute <dip>

dip 指定欲删除的负载均衡路由的目的 IP 地址

示例：

firewall>route del mroute 192.168.11.100

7. 显示路由：

route disp

示例：

firewall>route disp

4.4. ADSL 拨号 adsl

RG Wall 防火墙支持网卡通过 adsl 拨号获取地址，并且支持掉线重拨、时间调度、手动拨号等功能。adsl 拨号获取的地址可做为 nat 转换后的地址使用。

功能：本部分讲述 adsl 属性的设置、显示、连接和断开功能

1. 设置 adsl 属性

语法：

adsl set <interface> <username> <password> [type { manual | bootup | schedule time <name> }] [dyndomain { on domain <domainname> domainuser <name> domainpasswd <password> | off }] [autodial { on | off }] [active { on | off }]

参数说明：

interface：拨号所指定的网口

username：adsl 用户名

password：adsl 密码

manual：手工启动拨号连接

bootup：开机时启动拨号连接

schedule：定时启动拨号连接

time：时间调度名称，只有定时拨号时才能设置

dyndomain：开启或关闭动态域名，on 开启，off 关闭

domain：动态域名，只有开启动态域名时才能设置

domainuser: 动态域名的注册用户

domianpasswd：动态域名的用户密码

autodial：断开时是否自动连接，on 为自动连接，off 不进行自动连接。

active：是否在启动防火墙时启动 adsl 拨号功能，on 启用，off 不启用。

示例：

设置 adsl 为手动拨号，指定 fe2 网口通过 adsl 拨号获取 ip 地址，用户名和密码分别为 test 和 test123456，不启用动态域名，防火墙启动时启动 adsl 拨号功能。可进行如下设置：

firewall> adsl set fe2 test test123456 type manual active on

2. 手动连接和断开 adsl 功能

语法：

adsl { connect | disconnect }

参数说明

connect：手动连接

disconnect：手动断开

3. 显示 adsl 设置和状态

语法：

adsl disp [status]

参数说明：

status：可选参数，显示连接时动态信息。带 status 参数时，不连接时不显示任何信息。不带 status 参数时显示 adsl 设置的信息。

4.5. DHCP 配置

RG Wall 防火墙提供了强大的主机动态配置（DHCP）服务器功能，可以在复杂的网络拓扑中担当 dhcp 服务器的角色，以及 dhcp 客户端以及 dhcp 中继等。

功能：本部分讲述 dhcp 的各种配置，显示，启动，停止。

4.5.1. DHCP 服务器 dhcpserver

带格式的：项目符号和编号

添加 DHCP 域

语法：

dhcpserver add domain vpnclient { off <network> <netmask> | on <vpnmask> } <range> [gateway <gateway>] [dns <dns>] [domainname <domainname>] [comment <comment>]

参数说明：

vpnclient: 后面的 off | on 确定是否启用 vpn 客户端。若配置为 off，则需要输入 network 网络地址和掩码，若输入 on，则需要输入 vpn 客户端的掩码。

network：网络地址，必须是网段地址，而且需与防火墙网络设备在同一网段

netmask：网络掩码，与网络地址一起决定子网地址范围

range：地址范围，必须在地址资源中定义的。必须配置！

gateway：为 dhcp 客户端配置网关

domainname：为 dhcp 客户端配置域名（注意域名中不能有'.'，否则启动失败）

dns：为 dhcp 客户端配置 dns

comment：备注，0 到 256 个字符



当防火墙网口处于混合模式时，不支持 DHCP 服务器功能！

2. 配置静态 IP 地址

语法：

dhcpserver add static <hostname> <mac> <ip> [<comment>]

参数说明：

hostname：主机名称。

mac：主机 MAC 地址

ip：分配给此主机的 IP

3．删除 DHCP 域

功能：删除指定的 DHCP 域

dhcpserver del domain id <id>

参数说明：

Id：DHCP 域序号

4．删除静态 IP 地址

dhcpserver del static id <id>

5．设置 DHCP 域

语法：

dhcpserver set domain id <id> vpnclient { off <network> <netmask> | on <vpnmask> } < range <range> > [interface <interface>] [gateway <gateway>] [domainname <domainname>] [dns <dns>] [comment <comment>]

参数说明：

id：指定所要修改的 id

vpnclient: 后面的 off | on 确定是否启用 vpn 客户端。若配置为 off，则需要输入 network 网络地址和掩码，若输入 on，则需要输入 vpn 客户端的掩码。

network：设置网络 ip

netmask：设置网络掩码

range：地址范围，必须在地址资源中定义的。如不配置则和域同一范围

gateway：为 dhcp 客户端配置网关

domainname：为 dhcp 客户端配置域名（注意域名中不能有‘.’，否则启动失败）

dns：为 dhcp 客户端配置 dns。

comment：备注，0 到 256 个字符

6．设置静态 IP 地址

语法：

dhcpserver set static id <id> [hostname <hostname>] [mac <mac>] [ip <ip>] [comment <comment>]

参数说明：

id：指定所要修改的 id

hostname：指定请求服务的主机名

mac：指定请求服务的主机 mac 地址

ip：指定所分配的 ip

comment：备注，0 到 256 个字符

7．开启 DHCP 服务器

语法：

dhcpserver start

8．停止 DHCP 服务器

语法：

dhcpserver stop

9．显示 DHCP 设置

语法：

dhcpserver disp { domain | static | leases | state}

参数说明：

domain：显示域设置

static：显示静态设置

leases：显示分配状态

state：显示服务器当前状态

4.5.2. DHCP 客户端 dhcpclient

功能：

设置指定通过 dhcp 服务器获取 ip 地址的网络接口，以获取 dhcp 服务器所分配的 IP。

1、 开启 dhcp 客户端

语法：

dhcpclient <interface> on

参数说明：

Interface：网络接口名称，只能指定一个网络接口为 dhcp 客户端。

2、关闭客户端

dhcpclient off

2、 显示设置

语法：

dhcpclient disp [status]

参数说明：

status：可选参数，不输入显示 dhcp 客户端的哪个网口启用 dhcp 客户端，状态为 on 或者 off。输入 status 显示客户端当前状态，是 requesting 还是 connected。

4.5.3. DHCP 中继 dhcprelay

功能：设置 DHCP 中继，开启或关闭中继服务。

1. 设置 DHCP 中继

功能：

设置 DHCP 中继的相关数值

语法：

dhcprelay set server <ip> if <name>

参数说明：

server：指定 dhcp 服务器 IP

if：指定监听网口

2．开启/关闭 DHCP 中继

功能：

启动和停止 DHCP 中继功能

语法：

dhcprelay { start | stop }

3．显示 DHCP 中继设置

功能：

显示 DHCP 中继的有关配置

语法：

dhcprelay disp

5. VPN 配置

VPN 命令概述

VPN 命令行运行程序为 vpn，用来对 VPN 进行管理与设置。从功能上划分，总共分为以下几类：

基本参数管理、vpn 模块的启动与停止、VPN 客户端分组管理、远程 VPN 端点、自动 IKE 隧道管理、证书管理。

按照命令行的组织格式，总共分为以下几类子命令，它们分别为：

vpn set：该命令用来指定的 VPN 信息，可以用来设置网关、隧道的属性、也可以用来设置系统参数。

vpn add：该命令用来添加 VPN 信息，可以添加网关、隧道。

vpn show：该命令用来显示指定的内容，可以显示网关属性、隧道属性、系统参数和证书等。

vpn del：该命令用来删除指定的内容，可以删除网关、隧道、证书等。

vpn on/off：该命令用来启动或者停止 vpn 功能。

vpn status：该命令用来查看 vpn 状态。

vpn active/inactive：该命令用来启动或者停止指定的隧道。

VPN 命令行具有智能提示，如果用户不熟悉命令，在输入部分命令后，直接按回车键，系统就会提示下一步可能的输入或者需要输入内容的格式。例如，如果用户在命令行输入 vpn 加空格加？，按回车键，系统提示：

vpn on|off|status|add|show|set|del|active|inactive|connect ...

也就是说用户下一步可以输入 set，也可以输入 add，等等。

假如用户想要添加一个远程 VPN，但是不熟悉命令行，那么可以先输入 vpn，按回车键，参考提示，然后输入 vpn add，按回车键，就可以看到下面的提示：

vpn add remote|tunnel |group ...

表示在输入 vpn add 命令后可以输入 remote，tunnel，group 中的一个。它们分别表示要添加网关，添加隧道，添加拨号用户组。然后，用户输入 vpn add remote，再按回车键，就会得到网关的命令行格式提示。

5.1. VPN 基本配置

功能：

包括 VPN 基本参数的配置，显示，启动，停止。DHCP over IPSec 的相关配置。

5.1.1.设置基本参数

功能：

设置基本参数使用的命令是 vpn set default：

语法：

vpn set default [prekey <prekey>] [ikelifetime <ikelifetime>] [ipseclifetime <ipseclifetime>] [vpnstatus <on|off>]

参数说明：

参 数	描 述
<ikelifetime>	默认的第一阶段密钥生存期。单位可选，缺省单位为 sec，必须在［1200,86400］秒之间

<ipseclifetime>	默认的第二阶段密钥生存期。单位可选，缺省单位为 sec，必须在［1200,86400］秒之间
<prekey>	默认预共享密钥，长度 6-128 个字符，如果含有空格，需要用双引号括起来
< vpnstatus >	VPN 在重启时是否启动。

示例：

设置预共享密钥为 123456，默认的第一阶段密钥生存期 28800，默认的第二阶段密钥生存期是 3600。开机时启动 VPN

firewall>vpn set default prekey 123456 ikelifetime 28800 ipseclifetime 3600 vpnstatus on

5.1.2.显示基本参数

功能：

显示 vpn 的基本配置参数

语法：

vpn show default

基本参数使用的命令是 vpn show default

5.1.3.设置 DHCP over IPSec 信息

语法：

vpn set dhcp active{on|off} dhcpserver <dhcpserverip> interface <interface>

参数说明：

参　数	描　述
Active	是否启动 dhcp over ipsec。On，则启用 DHCP over IPSec 功能，可以为 VPN 客户端动态分配虚拟内部 IP 地址
<dhcpserver_ip>	为 VPN 客户端动态分配虚拟内部 IP 地址的 DHCP 服务器地址，如果使用本网关的 DHCP 服务器，该值填写为 127.0.0.1。
< interface >	从本网关到达 DHCP 服务器的网口，如果使用本网关的 DHCP 服务器，中继设备接口就是本地回环接口“lo”。

5.1.4.显示 DHCP over IPSec 信息

功能：

显示 dhcp 的相关信息

语法：

vpn show dhcp

示例：

firewall>vpn show dhcp

5.1.5.VPN 模块启动、停止

VPN 模块启动与停止使用的命令是 vpn on 和 vpn off。

功能：

启动和停止 vpn 功能

语法：

vpn on

vpn off

示例：

firewall>vpn on

firewall>vpn off

5.2. VPN 客户端分组

在使用 VPN 客户端访问单位网络时，可能存在很多出差、家庭办公、远程办公用户。需要为这些用户设置建立 VPN 的共享密钥、证书。如果为每一个远程用户单独设置远程 VPN 端点配置、自动 IKE 隧道，这样就增加了管理员的工作量。使用 VPN 客户端分组配置可以首先对众多具备一致属性的用户分组，减少在后续中的配置工作量。

5.2.1.添加 VPN 客户端分组

语法：

vpn add group name <groupname> idtype <psk|rsasig> [clientid <clientid>] [clientcert <clientcert>] [prekey <prekey>]

参数说明：

参　数	描　述
<groupname>	VPN 客户端分组名称。
idtype	认证类型（“psk”表示预共享密钥，“rsasig”表示证书）。

<clientid>	远程 VPN 客户端的用户 ID 列表，最多十个，用逗号分割各用户 id。
<clientcert>	远程 VPN 客户端的证书列表，最多十个，用逗号分割各用户证书。
<prekey>	远程 VPN 客户端的预共享密钥列表，最多十个，用逗号分割各用户预共享密钥，密钥长度 6-128 个字符，如果含有空格，需要用双引号括起来

示例：

添加一个有 zhang、wang、zheng 的分组，预共享密钥分别是 zhang123、wang4567、zheng8910。

firewall>vpn add group name group1 idtype psk clientid zhang,wang,zheng prekey zhang123,wang4567,zheng8910

5.2.2.设置 VPN 客户端分组

语法：

vpn set group name <groupname> idtype <psk|rsasig> [clientid <clientid>] [clientcert <clientcert>] [prekey <prekey>]

参数说明：

参 数	描 述
<groupname>	要修改的 VPN 客户端分组名称，不可修改。
idtype	认证类型（“psk”表示预共享密钥，“rsasig”表示证书）。

<clientid>	远程 VPN 客户端的用户 ID 列表，最多十个，用逗号分割各用户 id。
<clientcert>	远程 VPN 客户端的证书列表，最多十个，用逗号分割各用户证书。
<prekey>	远程 VPN 客户端的预共享密钥列表，最多十个，用逗号分割各用户预共享密钥，密钥长度 6-128 个字符，如果含有空格，需要用双引号括起来

示例：

设置一个名称为 group1 的客户端分组，将 zhang 的预共享密钥改为 test123456，成员仍为 zhang、wang、zheng。

firewall>vpn add group name group1 idtype psk clientid zhang,wang,zheng prekey test123456,wang4567,zheng8910

5.2.3.删除 VPN 分组

功能：

删除 vpn 分组

语法：

vpn del group <groupname>

参数说明：

groupname：要删除的 VPN 分组名称

5.3. 远程 VPN 配置

对于远程 VPN，按照远程 VPN 的地址类型，隧道认证方式（主模式、野蛮模式），认证类型（预共享密钥、证书），需要输入的内容也不一样。

5.3.1.添加远程 VPN

按照分类情况，添加远程 VPN 的命令分为七种情况：

在需要添加一个网关时，根据该远程 VPN 的类型选择相应的命令。

编号	地址类型	隧道认证方式	认证类型
1	动态类型	野蛮模式（aggr）	预共享密钥（psk）
2	（dynamic）		证书（rsasig）
3		主模式（main）	证书（rsasig）
4	静态类型	主模式（main）	预共享密钥（psk）
5	（static）		证书（rsasig）
6		野蛮模式（aggr）	预共享密钥（psk）
7			证书（rsasig）

可以将这些命令分为四类：添加野蛮模式、共享密钥的远程 VPN，添加野蛮模式、证书的远程 VPN，添加主模式、共享密钥的远程 VPN，添加主模式、证书的远程 VPN。

一般来说建立 VPN 客户端的隧道使用添加野蛮模式、共享密钥的远程 VPN。建立网关之间的隧道选择添加主模式、共享密钥的远程 VPN。如果使用证书一般用添加主模式、证书的远程 VPN。

1. 添加野蛮模式、共享密钥的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remoteid。这种情况主要使用于 VPN 客户端远程访问。

语法：

vpn add remote static|dynamic aggr psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localid <localid>] [remoteid <remoteid>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参 数	描 述
<remote name>	要添加网关的名称，要求唯一，以字母开头，由字母、数字和字符”-“、”_”组成，长度不超过 20 个字符。
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localid>	本地网关的设备 ID，本地身份标识符，必须是 1－15 位字母、数字、减号、下划线的组合且以字母开头。
<remoteid>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此项可以不写。必须是 1－15 位字母、数字、减号、下划线的组合且以字母开头。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}。
nat_t	是否启用 NAT 穿越。

<preshared key>	要添加网关的预共享密钥，长度范围为 6-128 个字符。
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间。
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

示例：

添加一个名称为 remotevpn 的客户端类型野蛮模式预共享密钥远程 VPN，ip 地址为 1.1.1.1，本地设备 ID 为 firewall，远程 VPN 用户 ID 是 zhang。预共享密钥为 abcdefg，ike 算法组件为 3des-sha-dh5，ike 生命周期为 7200 秒。DPD 的参数是可选的，如果不需要可以不写。

firewall>vpn add remote static aggr psk name remotevpn addr 1.1.1.1 localid firewall remoteid zhang prekey abcdefg ike 3des-sha-dh5 ikelifetime 7200

2. 添加野蛮模式、证书的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remotecert。一般不推荐用户使用这种方式，因为无论是静态地址，还是动态地址，都可以使用主模式和证书认证配合使用。

语法：

vpn add remote static|dynamic aggr psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike

{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参 数	描 述
<remote name>	要添加网关的名称，要求唯一，以字母开头，由字母、数字和字符"-"、"_"组成，长度不超过 20 个字符
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localcert>	本地网关的设备 ID
<remotecert>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此项可以不写。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

示例：

添加一个名称为 remotevpn 的客户端类型野蛮模式预共享密钥远程 VPN，ip 地址

为 0.0.0.0，本地证书 firewall，远程 VPN 证书 zhang，ike 算法组件为 3des-sha-dh5，ike 生命周期为 7200 秒。DPD 的参数是可选的，如果不需要可以不写。

firewall>vpn add remote client aggr psk name remotevpn addr 1.1.1.1 localcert firewall remotecert zhang ike 3des-sha-dh5 ikelifetime 7200

3. 添加主模式、共享密钥的远程 VPN

只能在静态地址，建立网关之间隧道情况下使用这种配置。这种情况主要使用建立企业分支机构之间的 VPN。

语法：

vpn add remote static main psk name <remote_name> addr <ip> prekey <prekey> [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参 数	描 述
<remote name>	要添加网关的名称，要求唯一，以字母开头，由字母、数字和字符”-“、”_”组成，长度不超过 20 个字符
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<prekey>	预共享密钥
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<preshared key>	要添加网关的预共享密钥，长度范围为 6-128 个字符

<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

示例：

添加一个名称为 shanghai 的网关类型主模式预共享密钥远程 VPN，ip 地址为 202.202.202.202，预共享密钥为 abcdefg，ike 算法组件为 3des-sha-dh5，ike 生命周期为 7200 秒。DPD 的参数是可选的，如果不需要可以不写。

firewall>vpn add remote static main psk name shanghai addr 202.202.202.202 prekey abcdefg ike 3des-sha-dh5 ikelifetime 7200

4. 添加主模式、证书的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remotecert。

语法：

vpn add remote static|dynamic main psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参　数	描　述
<remote name>	要添加网关的名称，要求唯一，以字母开头，由字母、数字和字符"-"、"_"组成，长度不超过 20 个字符
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localcert>	本地网关的设备 ID
<remotecert>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此项可以不写。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

示例：

添加一个名称为 remotevpn 的客户端类型野蛮模式预共享密钥远程 VPN，ip 地址为 0.0.0.0，本地证书 firewall，远程 VPN 证书 zhang，ike 算法组件为 3des-sha-dh5，ike 生命周期为 7200 秒。DPD 的参数是可选的，如果不需要可以不写。

firewall>vpn add remote dynamic main psk name remotevpn addr 1.1.1.1 localcert firewall remotecert zhang ike 3des-sha-dh5 ikelifetime 7200

5.3.2.设置远程 VPN

此部分主要讲述设置远程 vpn 网关，各参数说明和含义同添加远程 vpn，只是其中的 remote_name 参数需要指定，不能修改。

1. 设置野蛮模式、共享密钥的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remoteid。这种情况主要使用于 VPN 客户端远程访问。

语法：

vpn set remote static|dynamic aggr psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localid <localid>] [remoteid <remoteid>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参　数	描　述
<remote name>	要修改的网关名称，此参数不能修改。相当于远程 vpn 的索引。唯一标识。
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localid>	本地网关的设备 ID，本地身份标识符，必须是 1－15 位字母、数字、减号、下划线的组合且以字母开头。
<remoteid>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此

	项可以不写。必须是 1－15 位字母、数字、减号、下划线的组合且以字母开头。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<preshared key>	要添加网关的预共享密钥，长度范围为 8-128 个字符
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

2. 设置野蛮模式、证书的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remotecert。一般不推荐用户使用这种方式，因为无论是静态地址，还是动态地址，都可以使用主模式和证书认证配合使用。

语法：

vpn set remote static|dynamic aggr psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参 数	描 述
<remote name>	要修改的网关名称，此参数不能修改。相当于远程 vpn 的索引。唯一标识。
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localcert>	本地网关的设备 ID
<remotecert>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此项可以不写。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

3. 设置主模式、共享密钥的远程 VPN

只能在静态地址，建立网关之间隧道情况下使用这种配置。这种情况主要使用建

立企业分支机构之间的 VPN。

语法：

vpn set remote static main psk name <remote_name> addr <ip> prekey <prekey> [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参 数	描 述
<remote name>	要修改的网关名称，此参数不能修改。相当于远程 vpn 的索引。唯一标识。
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<prekey>	预共享密钥
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<preshared key>	要添加网关的预共享密钥，长度范围为 6-128 个字符
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

4. 设置主模式、证书的远程 VPN

可以使用静态地址或动态地址。如果类型是 VPN 客户端，可以使用 vpngroup 参数，不使用 remotecert。

语法：

vpn add remote static|dynamic main psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>]

参数说明：

参　数	描　述
<remote name>	要修改的网关名称，此参数不能修改。相当于远程 vpn 的索引。唯一标识。
<ip>	使用静态地址时，需要指定远程 VPN 的地址。
<groupname>	当远程 VPN 是 VPN 客户端时，可以使用预定义的分组。
<localcert>	本地网关的设备 ID
<remotecert>	远程 VPN 的设备 ID 或用户 ID，如果使用了 vpngroup，此项可以不写。
Ike	Ike 算法组件，可以取{{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}
nat_t	是否启用 NAT 穿越
<ikelifetime>	要添加网关的 ike 生命周期，单位为秒，必须在［1200,86400］之间
<dpddelay>	探测远程是否在线的时间间隔，单位为秒，允许配置的时间

	范围[5，180]。0 表示不启用 DPD。
<dpdtimeout>	探测远程是否在线的超时周期。在发出探测后，如果超过这个时间还未收到回应，则认为隧道远端端点已经离线。单位为秒，允许配置的时间范围[5，600]。0 表示不启用 DPD。

5.3.3.显示远程 VPN 网关

功能：

显示远程 vpn 网关的命令为 vpn show remote …，该命令用来显示指定网关的详细属性。

语法：

vpn show remote {all | <remotename>}

参数说明：

参　数	描　述
<remote name>	要显示的网关的名称
all	当用 all 代替网关名称时，用来显示所有的网关。

示例：

显示所有网关的信息：

firewall>vpn show remote all

显示网关 cl_test 的信息：

firewall>vpn show remote cl_test

> 注意：由于 all 是系统所采用的关键字，因此不能用 a，al，all 来为网关等命名，否则会引起歧义。

5.3.4.删除网关

功能：

该命令用来删除指定的网关。在删除网关的同时，系统会自动删除所有引用该网关的隧道。

语法：

vpn del remote <remotename>

参数说明：

参　数	描　述
<remote name>	要删除的网关的名称

示例：

删除网关 cl_test：

firewall>vpn del remote cl_test

> 由于 all 是系统所采用的关键字，因此不能用 a，al，all 来为网关等命名，否则会引起歧义。

5.3.5.网关生效

网关生效的命令为 vpn active remote …，该命令用来使指定网关生效。

语法：

vpn active remote <remotename>

参数说明：

参　数	描　述
<remote name>	要生效的网关的名称

示例：

网关 cl_test 生效：

firewall>vpn active remote cl_test

5.3.6.网关失效

网关失效的命令为 vpn inactive remote …，该命令用来使指定网关生效。

语法：

vpn inactive remote <remotename>

参数说明：

参 数	描 述
<remote name>	要失效的网关的名称

示例：

网关 cl_test 失效：

firewall>vpn inactive remote cl_test

网关失效的同时，引用本网关的隧道也相应失效。

5.4. 隧道配置

5.4.1.添加隧道

语法：

vpn add tunnel name <tunnelname> local <local> remote <remote> [auth {esp|ah|comp}]

[ipsec <{3des|aes128|aes256|null}-{md5|sha1}>] [pfs on|off dh_group <1|2|5>] [ipseclifetime <ipseclifetime>] proxy_localip <proxy_localip> proxy_localmask <proxy_localmask> proxy_remoteip <proxy_remoteip> proxy_remotemask < proxy_remotemask>

参数说明：

参 数	描 述
<tunnelname>	要添加的隧道名称，必填项
<local>	本地 ip 地址，必填项
<remote>	使用远端网关名字，必填项
auth	数据包封装形式，esp 或者 ah。
ipsec	数据通信和认证时支持的加密和认证算法选择。多选项，可选内容为：3des-md5，3des-sha1，aes128-md5，aes128-sha1，aes256-md5，aes256-sha1，null-md5，null-sha1。用逗号分隔多个协商提案。
pfs	是否完美向前保密，on 或者 off。
dh_group	在使用 pfs 时，支持的 DH 群 1，2，5。单选。
<ipseclifetime>	Ipsec 生命周期，单位为秒，取值范围 1200-86400。
<proxy_localip>	本地保护子网
<proxy_localmask>	本地保护子网掩码
<proxy_remoteip>	远程保护子网
< proxy_remotemask>	远程保护子网掩码

5.4.2.设置隧道

语法：

vpn set tunnel name <tunnelname> { [local <localaddr>] [remote <remotename>] [auth {esp|ah}] [ipsec <{3des|aes128|aes256|null}-{md5|sha1}>] [pfs {on [dh_group {1|2|5}] |off}] [ipseclifetime <ipseclifetime>] [proxy_localip <proxy_localip>] [proxy_localmask <proxy_localmask>] [proxy_remoteip <proxy_remoteip>] [proxy_remotemask < proxy_remotemask>]}

参数说明：

参 数	描 述
<tunnelname>	要设置的隧道名称，不能修改
<local>	本地 ip 地址
<remote>	使用远端网关名字
auth	数据包封装形式，esp 或者 ah。
ipsec	数据通信和认证时支持的加密和认证算法选择。多选项，可选内容为：3des-md5，3des-sha1， aes128-md5，aes128-sha1，aes256-md5，aes256-sha1，null-md5，null-sha1。用逗号分隔多个协商提案。
pfs	是否完美向前保密，on 或者 off。
dh_group	在使用 pfs 时，支持的 DH 群 1，2，5。单选。
<ipseclifetime>	Ipsec 生命周期，单位为秒，取值范围 1200-86400。
<proxy_localip>	本地保护子网
<proxy_localmask>	本地保护子网掩码
<proxy_remoteip>	远程保护子网

< proxy_remotemask>	远程保护子网掩码

5.4.3.显示隧道

显示隧道的命令为 vpn show tunnel all|tunnelname…，该命令用来显示指定隧道的详细属性。

语法：

vpn show tunnel {all | <tunnelname>}

参数说明：

参　数	描　述
<tunnelname>	要显示的隧道的名称
all	当用 all 代替网隧道名称时，用来显示所有的隧道。

示例：

显示所有隧道的信息：

vpn show tunnel all

显示隧道 cl_test 的信息：

vpn show tunnel cl_test

5.4.4.删除隧道

功能：

该命令用来删除指定的隧道。

语法：

vpn del tunnel <tunnelname>

参数说明：

参　数	描　述
<tunnelname>	要删除的隧道的名称

示例：

删除隧道 cl_test：

firewall>vpn del tunnel cl_test

5.4.5.隧道生效

隧道生效的命令为 vpn active tunnel…，该命令用来使指定隧道生效。

语法：

vpn active tunnel <tunnelname>

参数说明：

参　数	描　述
<tunnel name>	要生效的隧道的名称

示例：

隧道 cl_test 生效：

firewall>vpn active tunnel cl_test

5.4.6.隧道失效

隧道失效的命令为 vpn inactive tunnel…，该命令用来使指定隧道失效。

语法：

vpn inactive tunnel <tunnelname>

参数说明：

参　数	描　述
<tunnel name>	要失效的隧道的名称

示例：

隧道 cl_test 失效：

firewall>vpn inactive tunnel cl_test

5.5. VPN 设备

5.5.1.添加虚设备

功能：

增加一个 vpn 虚设备，一个虚设备对应一个隧道，供添加路由时引用。

语法：

vpndev add <dev_name> <tunnel_name> [<comment>]

参数说明：

<dev_name>：设备名称

<tunnel_name>：隧道名称

<comment>：备注

5.5.2.编辑虚设备

功能：

修改虚设备

语法：

vpndev set <dev_name> { [tunnel <tunnel_name>] [comment <comment>] }

参数说明：

dev_name：设备名称，不能修改

tunnel_name：隧道名称

comment：备注

5.5.3.删除虚设备

功能：

删除一个虚设备

语法：

vpndev del <dev_name>

参数说明：

dev_name：要删除的设备名称

5.5.4.显示虚设备

功能：

显示虚设备的信息

语法：

vpndev disp

5.6. 证书管理

证书的添加需要通过 Web 管理来完成，在命令行方式下，只能进行证书的显示和

删除。证书分为三类：ca 证书、对端证书 remote 和本地证书 local。

5.6.1.显示证书

语法：

vpn show cert {<ca>|<remote>|<local>}

参数说明：

参　数	描　述
<ca>	显示所有的 ca 证书。
<remote>	显示所有的远端证书。
<local>	删除所有的本地证书。

示例：

显示所有的本地证书：

firewall>vpn show cert local

5.6.2.删除证书

功能：

用来删除指定的证书。

删除证书的命令按照证书的分类分为三个，分别用来删除 ca 证书、对端证书、本地证书。

如果某个证书被引用，则无法删除。而且，如果指定的证书类型与证书的实际类型不符，也无法删除该证书。

语法：

vpn del cert ca {<certname>}，该命令用于删除指定的 ca 证书。

vpn del cert remote {<certname>}，该命令用于删除指定的对端证书。

vpn del cert local {<certname>}，该命令用于删除指定的本地证书。

参数说明：

参 数	描 述
<certname>	要删除的证书名称。

示例：

删除本地证书 cer1：

firewall>vpn del cert local cer1

5.7. PPTP/L2TP 配置

防火墙支持 PPTP/L2TP 协议的 VPN。

5.7.1.服务器配置 pptpserver

1. 设置 PPTP 服务

语法：

pptpserver set iprange <name> encrypt { 40 | 56 | 128 } auth { [chap] [chapms] [chapms-v2] } [dns <ip>+ |none] [wins <ip>+|none]

参数说明：

iprange：设置 IP 地址段，必须是地址资源。

<name>：资源定义中的地址名称，必须是一个网段中的连续地址。并且不能包含最后一位是 0 和 255 的地址。

encrypt：加密强度，可选数值是 40、56 和 128 位

auth：认证方式，选 chap、chapms、chapms-v2 的至少一种。

dns：为客户端指定 dns 服务器

IP：dns 的 IP， 最多 2 个，可以不设置，输入 none

wins：wins 服务器

IP：wins 的 IP， 最多 2 个，可以不设置，输入 none

示例：

配置 pptpserver，iprange 为已定义好的 pptpip, 加密强度为 128 位，认证方式选 chap, chapms, dns ip 设置为 202.1.1.1, wins 值为 210.1.1.1

firewall>pptpserver set iprange pptpip encrypt 128 auth chap chapms dns 202.1.1.1 wins 210.1.1.1

2．启动和停止 pptp 服务器

pptpserver start

pptpserver stop

3．显示 PPTP 服务器设置

pptpserver disp

5.7.2.拨号用户 pptpuser

1．添加 PPTP 用户

语法：

pptpuser add <name> <password> [<ip>] [<comment>]

参数说明：
<name>：PPTP 用户名称
<password>：用户密码 6~15 个字符
<ip>：分配给用户的 IP 地址
<comment>：备注，最多 255 个字符

2. 编辑 PPTP 用户

语法：

pptpuser set <name> { [password <password>] [ip <ip> | none] [comment <comment>] }
pptpuser del <name>
pptpuser disp [online] [<name>]
参数说明：
<name>：要修改的 PPTP 用户名称
password：用户新密码 6~15 个字符
<ip>：分配给用户的 IP 地址，none 表示不修改。
<comment>：备注，最多 255 个字符

3. 删除 PPTP 用户

语法：

pptpuser del <name>

参数说明：
<name>：要删除的 PPTP 用户名称

4. 显示 PPTP 用户

语法：

pptpuser disp [online] [<name>]

参数说明：

online：显示所有在线 PPTP 用户

name：显示用户名为 name 的参数信息。

6. 对象定义

本章描述各种对象的定义方法，这些对象定义可供安全规则使用，包括：地址列表、地址组、服务器地址、地址池、服务列表、服务组、代理服务、邮件过滤、用户列表、用户组、时间列表、时间组、连接限制、带宽策略、URL过滤等。

注意 **所有对象都遵循以下两条准则（1）不能删除被引用的对象，即只要该对象被其它规则、对象或者设置引用到了，那么就不能删除该对象；（2）所有对象都可以被修改，包括被引用的对象。在下面就不重复以上两条规则了。**

注意 **所有对象名称都不能使用保留字，本系统中的保留字及含义如下表所示：**

保留字	含义
any	表示任意，如任意 IP 地址、任意服务
none	表示不使用

6.1. 地址 defaddr

功能：设置地址列表。可被地址组、安全规则、用户、用户组引用。

语法：

defaddr add <name> <ip> [<comment>]　　添加地址对象

defaddr set <name> { [ip <ip>] [comment <comment>] }　　修改地址对象

defaddr del <name>　　删除地址对象

defaddr disp　　显示地址列表中的所有地址

defaddr disp <name> 显示特定地址对象的详细信息

 这里的 IP 地址可以使用单个 IP 地址、IP 地址/子网掩码和 IP 地址段

示例：

firewall>defaddr add dmz 192.168.10.100 “web server”

firewall>defaddr set dmz ip 192.168.10.101/255.255.255.255 comment “new web server”

firewall>defaddr disp

firewall>defaddr disp dmz

firewall>defaddr del dmz

6.2. 地址组 defaddrgrp

功能：设置地址组。

语法：

defaddrgrp add <name> [<comment>] 添加地址组对象

defaddrgrp set <name> <comment> 修改地址组对象

defaddrgrp addmbr < name> <name>+ 为地址组添加成员

成员只能是地址列表中的，同一成员可以加入不同地址组

defaddrgrp delmbr < name> <name>+ 从地址组中删除成员

defaddrgrp delallmbr <name> 删除所有的成员

defaddrgrp disp [<name>] 显示地址组

defaddrgrp del <name> 删除地址组

示例：

firewall>defaddrgrp add trustgrp “inner subnet”

firewall>defaddrgrp set trustgrp “new inner subnet”

把地址 trust1、trust2、trust3 加入到地址组 trustgrp1 中，可使用如下命令：

firewall>defaddrgrp addmbr trustgrp trust1 trust2 trust3

显示所有地址组，可使用以下命令：

firewall>defaddrgrp disp

显示地址组 trustgrp 的详细信息，可使用以下命令：

firewall>defaddrgrp disp trustgrp

从地址组 trustgrp 中删除地址 trust2，可以使用如下命令：

firewall>defaddrgrp delmbr trustgrp trust2

删除地址组 trustgrp 中的所有成员，可以使用如下命令：

firewall>defaddrgrp delallmbr trustgrp

提示：输入示例中的命令之前，必须先定义地址 trust1、trust2、trust3（请查阅 defaddr 命令）

6.3. 服务器地址 defsrvaddr

功能：设置服务器地址。用于反向 NAT（端口映射、IP 映射）规则中的内部地址，以实现内部服务器的负载均衡功能。

语法：

defsrvaddr add <name> ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>]]]]]]]] [comment <comment>]

defsrvaddr set <name> { [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>]]]]]]]]] [comment <comment>] }

defsrvaddr del <name>

defsrvaddr disp [<name>]

参数说明：

name	设置服务器地址定义的名字
ip	设置服务器的 IP 地址，仅能使用单个 IP 地址
weight	设置服务器的权重，有效值为 0 至 65535，可选参数，默认为 1
comment	设置服务器地址定义的注释，可选参数，默认为空



在一个服务器地址定义中最多可以设置 8 个服务器。

示例：

firewall> defsrvaddr add sa1 ip 192.168.100.1 weight 10 ip 192.168.100.2 weight 20 comment “server address 1”

firewall> defsrvaddr set sa1 ip 192.168.100.1 weight 10 ip 192.168.100.2 weight 20 comment “new server defaddr 1”

firewall> defsrvaddr disp

firewall> defsrvaddr disp sa1

firewall> defsrvaddr del sa1

6.4. NAT 地址池 defaddrpool

功能：设置地址池。主要用于双向 NAT（NAT、端口映射、IP 映射）中的源地址转

换。每个 NAT 地址池不超过 254 个 IP，所有 NAT 地址池中不同 IP 地址的总数不超过 4096 个。IP 地址不能跨网段。不同的地址池定义之间不能有相同的 IP 地址。

语法：

defaddrpool add <name> <ip> [comment <comment>]

defaddrpool set <name> { [ip <ip>] [comment <comment>] }

defaddrpool del <name>

defaddrpool disp [<name>]

参数说明：

name	设置 NAT 地址池定义的名字
ip	设置 NAT 地址池定义的 IP 地址，可以使用单个 IP 地址、IP 地址/子网掩码、IP 地址段
comment	设置 NAT 地址池定义的注释，可选参数，默认为空

注意 地址池定义的 IP 地址不能与网络接口 HA 和 MNG 上的 IP 地址在同一子网；每个 NAT 地址池定义中的 IP 地址数量不能超过 254 个，所有 NAT 地址池中不同 IP 地址的总数不超过 4096 个。

示例：

firewall>defaddrpool add sat1 192.168.1.10:192.168.1.20 comment “SAT defaddr 1”

firewall>defaddrpool set sat1 192.168.1.30:192.168.1.40 comment “new SAT defaddr 1”

firewall>defaddrpool disp

firewall>defaddrpool disp sat1

firewall>defaddrpool del sat1

6.5. 服务 defsvc

功能：设置服务列表。包括：动态协议（FTP/H.323/SQLnet）、普通协议、ICMP 协议等。

1. FTP 服务：

语法：

defsvc add <name> ftp <port> [comment <comment>]　　添加 ftp 服务

defsvc set <name> ftp <port>　　修改 ftp 服务

示例：

firewall>defsvc add myftp_1 ftp 2021 comment “FTP 1”

firewall>defsvc set myftp_1 ftp 3021

2. H.323 服务：

语法：

defsvc add <name> h323 <port> [comment <comment>]　　添加 h323 服务

defsvc set <name> h323 <port>　　修改 h323 服务

示例：

firewall>defsvc add my_h323_1 h323 1720 comment “H.323 1”

firewall>defsvc set my_h323_1 h323 2720

3. SQLNET 服务：

语法：

defsvc add <name> sqlnet <port> [comment <comment>]　　添加 SQLNET 服务

defsvc set <name> sqlnet <port>　　修改 SQLNET 服务

示例：

firewall>defsvc add my_sqlnet_1 sqlnet 1521 comment "SQLNET 1"

firewall>defsvc set my_sqlnet_1 sqlnet 2521

4. ICMP 服务：

语法：

defsvc { add | set } <name> icmp [type { 0 | 3 [code { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 }] | 4 | 5 [code { 0 | 1 | 2 | 3 }] | 8 | 9 | 10 | 11 [code { 0 | 1 }] | 12 [code { 0 | 1 }] | 13 | 14 | 17 | 18 }] [comment <comment>]

参数说明：

type 设置 ICMP 协议的类型，可选参数，默认为"any"

code 设置 ICMP 协议的 code，可选参数，默认为"any"

示例：

firewall>defsvc add my_icmp1 icmp type 3 code 10 comment "ICMP 1"

firewall>defsvc set my_icmp1 icmp type 0

5. 自定义服务（IP 协议）：

语法：

defsvc add | set <name> proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto{ { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> }]]]]]]] [comment <comment>]

参数说明：

name 设置服务定义的名字

protocol	设置服务项的协议号，可以使用“TCP”、“UDP”、数字（不能为1、6、17）
sp	当服务项的协议号为“TCP”或“UDP”时，设置源端口，可以使用单个端口、端口段、“any”
dp	当服务项的协议号为“TCP”或“UDP”时，设置目的端口，可以使用单个端口、端口段、“any”
comment	设置服务定义的注释，可选参数，默认为空



在一个普通 IP 协议的服务定义中最多可以设置 8 个服务项。

示例：

firewall>defsvc add common1 proto tcp 1000 7000 proto udp any any proto 10 comment “common 1”

firewall>defsvc set common1 proto tcp 2000 7000 proto 10

6. 删除服务：

语法：

defsvc del <name>

示例：

firewall>defsvc del my_ftp1

firewall>defsvc del my_h323_1

firewall>defsvc del my_sqlnet_1

firewall>defsvc del my_icmp_1

firewall>defsvc del common1

7. 修改服务的注释信息：

语法：

defsvc set <name> comment <comment>

示例：

firewall>defsvc set my_icmp_1 comment “new icmp 1”

firewall>defsvc set my_ftp1 comment “new ftp 1”

firewall>defsvc set common1 comment “new common 1”

8. 显示服务信息：

语法：

defsvc disp { dynamic | icmp | common | <name> }

参数说明：

dynamic　　仅显示所有动态服务信息，包括 ftp、h323、sqlnet 等服务

icmp　　仅显示所有 icmp 服务信息

common　　仅显示所有自定义服务（IP 协议）信息

<name>　　显示指定名称的服务详细信息

示例：

firewall>defsvc disp dynamic

firewall>defsvc disp icmp

firewall>defsvc disp common

firewall>defsvc disp my_ftp1

6.6. 服务组 defsvcgrp

功能：设置服务组。必须是已定义的服务。

语法：

defsvcgrp add <name> [comment <comment>]　　添加服务组

defsvcgrp set <name> comment <comment> 修改服务组

defsvcgrp addmbr <name> <name>+ 往服务组中增加成员

defsvcgrp delmbr < name> <name>+ 删除服务组中指定的成员

defsvcgrp delallmbr <name> 删除服务组中所有的成员

defsvcgrp del <name> 删除指定的服务组

defsvcgrp disp [<name>] 显示服务组

示例：

firewall>defsvcgrp add sg1 comment “defsvc group 1”

firewall>defsvcgrp set sg1 comment “new defsvc group 1”

要把服务 my_ftp1、common1 和 my_icmp_1 加入到服务组 sg1 中，可执行如下命令：

firewall>defsvcgrp addmbr sg1 my_ftp1 common1 my_icmp_1

显示所有服务组的信息

firewall>defsvcgrp disp

显示指定服务组的详细信息

firewall>defsvcgrp disp sg1

要从组 sg1 中删除服务 common1，可执行如下命令：

firewall>defsvcgrp delmbr sg1 common1

删除服务组 sg1 中的所有成员

firewall>defsvcgrp delallmbr sg1

提示：必须首先定义服务my_ftp1、common1 和my_icmp_1（请查阅 30 页的defsvc命令）。

6.7. 代理 defproxy

功能：设置代理服务。

1. 设置 HTTP 代理服务：

语法：

defproxy set http { [port <port>] [java { permit | deny }] [javascript { permit | deny }] [activex { permit | deny }] }

参数说明：

port	设置 HTTP 代理服务端口（TCP）
java	设置是否允许 Java
javascript	设置是否允许 JavaScript
activex	设置是否允许 ActiveX

示例：

firewall>defproxy set http port 80 java permit javascript permit activex permit

2. 设置 FTP 代理服务：

语法：

defproxy set ftp { [port <port>] [get { permit | deny }] [put { permit | deny }] [multi { permit | deny }] }

参数说明：

port	设置 FTP 代理服务端口（TCP）
get	设置是否允许使用 get 命令
put	设置是否允许使用 put 命令
multi	设置是否允许使用多线程

示例：

firewall>defproxy set ftp port 21 get permit put permit multi permit

3. 设置 TELNET 代理服务：

语法：

defproxy set telnet port <port>

参数说明：

port	设置 TELNET 代理服务端口（TCP）

示例：

firewall>defproxy set telnet port 23

4. 设置 SMTP 代理服务：

语法：

defproxy set smtp { [port <port>] [domain <domainname>+] [server <domainname>] [maildomain <domainname>+][mailserver <ip>+][maxlength <number>] [maxreceiver <number>] [sendinterval <number>] [sendamount <number.]}

参数说明：

port	设置 SMTP 代理服务端口（TCP）
domain	设置代理域名
server	设置 SMTP 服务器的真实域名
maildomain	设置邮件域名
mailserver	设置内部邮件服务器
maxlength	设置每封邮件的最大长度，有效值为 0 至 10240（千字节）
maxreceiver	设置每封邮件的最多接收人数，有效值为 1 至 99

sendinterval　　设置发信周期，有效值为 1－1440 分钟

sendamount　　设置一个周期内的发信封数，有效值为 1－144000

示例：

firewall>defproxy set smtp port 25 domain sec.com server sec.com maildomain sec.com mailserver 10.50.10.11 maxlength 5000 maxreceiver 10 sendinterval 10 sendamount 10

5. 设置 POP3 代理服务：

语法：

defproxy set pop3 { [port <port>] [maxlength <number>] }

参数说明：

port　　设置 POP3 代理服务端口（TCP）

maxlength　　设置每封邮件的最大长度，有效值为 0 至 10240（千字节）

示例：

firewall>defproxy set pop3 port 110 maxlength 5000

6. 显示预定义代理服务：

语法：

defproxy disp default

示例：

firewall>defproxy disp default

7. 用户自定义代理服务：

语法：

defproxy add custom <name> port <port> [comment <comment>]

defproxy set custom <name> { [port <port>] [comment <comment>] }

defproxy disp custom

defproxy del custom <name>

参数说明：

<name>	设置用户自定义代理服务的名字
port	设置用户自定义代理服务的端口（TCP）
comment	设置用户自定义代理服务的注释，可选参数，默认为空

示例：

firewall>defproxy add custom cp1 port 7000 comment “custom defproxy 1”

firewall>defproxy set custom cp1 port 3000 comment “new custom defproxy 1”

firewall>defproxy disp custom

firewall>defproxy del custom cp1

6.8. 邮件过滤 defmail

功能：对收、发邮件的各区域（收件人、发件人、附件等等）进行关键字过滤，在相应区域内含有关键字的邮件将被过滤掉。

on	表示对该类型的关键字进行匹配
off	表示对该类型的关键字不进行匹配

1. 发送邮件的发件人：

defmail set smtp sender [<keyword>+]

defmail { on | off } smtp sender

2. 发送邮件的收件人：

defmail set smtp receiver [<keyword>+]

defmail { on | off } smtp receiver

3. 发送邮件的主题：

defmail set smtp subject [<keyword>+]

defmail { on | off } smtp subject

4. 发送邮件的内容：

defmail set smtp content [<keyword>+]

defmail { on | off } smtp content

5. 发送邮件的附件：

defmail set smtp attach [<keyword>+]

defmail { on | off } smtp attach

6. 接收邮件的发件人：

defmail set pop3 sender [<keyword>+]

defmail { on | off } pop3 sender

7. 接收邮件的收件人：

defmail set pop3 receiver [<keyword>+]

defmail { on | off } pop3 receiver

8. 接收邮件的主题：

defmail set pop3 subject [<keyword>+]

defmail { on | off } pop3 subject

9. 接收邮件的附件：

defmail set pop3 attach [<keyword>+]

defmail { on | off } pop3 attach

示例：

firewall>defmail set smtp sender “keyword 1” “keyword 2”

firewall>defmail on sender

firewall>defmail set smtp receiver “keyword 1” “keyword 2”

firewall>defmail on smtp receiver

firewall>defmail set pop3 attachment “keyword 1” “keyword 2”

firewall>defmail off pop3 attachment

10. 显示邮件内容过滤设置：

defmail disp smtp　　显示发送邮件的过滤设置

defmail disp pop3　　显示接收邮件的过滤设置

6.9. 时间 deftime

功能：设置时间定义。包括：一次性时间定义和周循环时间定义。被时间组、安全规则、用户、用户组引用。

1. 一次性时间定义：

语法：

deftime add <name> once < date> < time> < date> < time> [comment <comment>]

deftime set <name> once { [<date> <time> <date> <time>] [comment <comment>] }

deftime del <name>

deftime disp [<name>]

参数说明：

name　　指定时间定义的名字

date　　日期，格式为 yyyy/mm/dd

time　　时间，格式为 hh:mm:ss

comment　　指定时间定义的注释，可选参数，默认为空

 开始时间必须早于结束时间。

示例：

firewall>deftime add rest_time once 2005/10/01 00:00:00 2005/10/03 23:59:59 comment “guoqingjie3tian”

firewall>deftime set rest_time once 2005/10/01 00:00:00 2005/10/07 23:59:59 comment “guoqingjie7tian”

2. 周循环时间定义：

语法：

deftime add <name> week { [sun <time>] [mon <time>] [tue <time>] [wed <time>] [thu <time>] [fri <time>] [sat <time>] } [comment <comment>]

deftime set <name> week { [sun <time>] [mon <time>] [tue <time>] [wed <time>] [thu <time>] [fri <time>] [sat <time>] [comment <comment>] }

参数说明：

name	指定时间定义的名字
sun	指定周日的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
mon	指定周一的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
tue	指定周二的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
wed	指定周三的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
thu	指定周四的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
fri	指定周五的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
sat	指定周六的时间段，格式为 hh:mm:ss-hh:mm:ss 或 hh:mm-hh:mm
comment	指定时间定义的注释，可选参数，默认为空

 开始时间必须早于结束时间。未指定时间段的日子将会被清空。

示例：

firewall>deftime add work_time week mon 09:00-18:00 tue 09:00-18:00 wed 09:00-18:00 thu 09:00-18:00 fri 09:00-18:00 comment “work time”

firewall>deftime set work_time week mon 10:00-18:00 tue 10:00-18:00 wed 10:00-18:00 thu 10:00-18:00 fri 09:00-18:00 comment “new work time”

3. 删除时间定义：

deftime del <name>

4. 显示时间定义：

deftime disp 显示时间列表

deftime disp <name> 显示指定时间定义的详细内容

6.10. 时间组 deftimegrp

语法：

deftimegrp add <name> [comment <comment>] 添加时间组

deftimegrp set <name> comment <comment> 修改时间组

deftimegrp addmbr < name> <name>+ 往时间组里添加成员

deftimegrp delmbr < name> <name>+ 从时间组里删除成员

deftimegrp delallmbr <name> 删除时间组中的所有成员

deftimegrp del <name> 删除时间组

deftimegrp disp [<name>] 显示时间组

参数说明：

name 设置时间组的名字

name　　　设置时间调度的名字

comment　　设置时间组定义的注释，可选参数，默认为空

示例：

firewall>deftimegrp add timegroup1 comment “time group 1”

firewall>deftimegrp set timegroup1 comment “new time group 1”

要把时间 t1、t2、t3 加入到时间组 timegroup1，可使用如下命令：

firewall>deftimegrp addmbr timegroup1 t1 t2 t3

要把时间 t2 从 timegroup1 中删除，可使用如下命令：

firewall>deftimegrp delmbr timegroup1 t2

firewall>deftimegrp del timegroup1

提示：输入示例中的命令之前，必须先定义时间对象 t1、t2、t3（请查阅 deftime 命令）。

6.11. 保护主机 hostprotect

功能：设置保护主机参数。包括：源 IP 地址、目的 IP 地址、连接控制、周期、阻断时间等。

1. 添加保护主机：

语法：

hostprotect add <name> sa <ip> da <ip> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>]

参数说明：

name　　　设置保护主机的名字

sa　设置保护主机的源 IP 地址，可以是一个 IP 地址或者网段

da　　　　设置保护主机的目的 IP 地址

newconn　　开启限制新建连接的功能

type　　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　　设置阻断时间，必须大于等于 period

concurrent　开启限制并发连接的功能

comment　　设置保护主机的注释，可选参数，默认为空

示例：

firewall>hostprotect add webcnct sa 192.168.10.0/255.255.255.0 da 10.50.10.1 newconn on type each 100 60 70 concurrent on type share 100 comment “new WEB protection”

2. 修改保护主机：

语法：

hostprotect set <name> { [sa <ip>] [da <ip>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] }

参数说明：

name　　　设置保护主机的名字

sa　设置保护主机的源 IP 地址，可以是一个 IP 地址或者网段

da　　　　设置保护主机的目的 IP 地址

newconn　　开启限制新建连接的功能

type　　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　设置阻断时间，必须大于等于 period

concurrent　开启限制并发连接的功能

comment　　设置保护主机的注释，可选参数，默认为空

示例：

firewall>hostprotect set webcnct sa 192.168.10.0/255.255.255.0 da 10.50.10.1 newconn on type each 100 60 70 concurrent on type share 100 comment “new WEB protection”

3. 显示保护主机：

语法：

hostprotect disp [<name>]

参数说明：

name　　保护主机的名字

示例：

firewall>hostprotect disp webcnct

4. 删除保护主机：

语法：

hostprotect del <name>

参数说明：

name　　保护主机的名字

示例：

firewall>hostprotect del webcnct

5. 清空保护主机：

语法：

hostprotect clean
示例：

firewall>hostprotect clean

6.12. 保护服务 svcprotect

功能：设置保护服务参数。包括：源 IP 地址、目的 IP 地址、目的端口、连接数量、周期、阻断时间等。

1. 添加保护服务：

语法：

svcprotect add <name> sa <ip> da <ip> dp <port> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>]

参数说明：

name　　设置保护服务的名字

sa　设置保护服务的源 IP 地址，可以是一个 IP 地址或者网段

da　　设置保护服务的目的 IP 地址

dp　　设置保护的端口号，有效值为 1 至 65535

newconn　　开启限制新建连接的功能

type　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　设置阻断时间，必须大于等于 period

concurrent　　开启限制并发连接的功能

comment　　设置保护服务的注释，可选参数，默认为空

示例：

firewall>svcprotect add webcnct sa 192.168.10.0/255.255.255.0 da 10.50.10.1 dp 80 newconn on type each 100 60 70 concurrent on type share 100 comment “new service protection”

2. 修改保护服务：

语法：

svcprotect set <name> { [sa <ip>] [da <ip>] [dp <port>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] }

参数说明：

name　　设置保护服务的名字

sa　设置保护服务的源 IP 地址，可以是一个 IP 地址或者网段

da　　设置保护服务的目的 IP 地址

dp　　设置保护的端口号，有效值为 1 至 65535

newconn　　开启限制新建连接的功能

type　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　设置阻断时间，必须大于等于 period

concurrent　　开启限制并发连接的功能

comment　　设置保护服务的注释，可选参数，默认为空

示例：

firewall>svcprotect set webcnct sa 192.168.10.0/255.255.255.0 da 10.50.10.1 dp 80 newconn on type each 100 60 70 concurrent on type share 100 comment “new service protection”

3. 显示保护服务：

语法：

svcprotect disp [<name>]

参数说明：

name　　保护服务的名字

示例：

firewall>svcprotect disp webcnct

4. 删除保护服务：

语法：

svcprotect del <name>

参数说明：

name　　保护服务的名字

示例：

firewall>svcprotect del webcnct

5. 清空保护服务：

语法：

svcprotect clean

示例：

firewall>svcprotect clean

6.13. 限制主机 hostlimit

功能：设置限制主机参数。包括：源 IP 地址、连接数量、周期、阻断时间等。

1. 添加限制主机：

语法：

hostlimit add <name> sa <ip> { [newconn { on { type { each| share} <connect> <period> <block> } | off }] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>]

参数说明：

name 设置限制主机的名字

sa 设置限制主机的源 IP 地址，可以是一个 IP 地址或者网段

newconn 开启限制新建连接的功能

type 设置独占模式或者共享模式

connect 设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period 设置周期，有效值为 1 至 3600（秒）

block 设置阻断时间，必须大于等于 period

concurrent 开启限制并发连接的功能

comment 设置限制主机的注释，可选参数，默认为空

示例：

firewall>hostlimit add webcnct sa 192.168.10.0/255.255.255.0 newconn on type each 100 60 70 concurrent on type share 100 comment “new WEB limition”

2. 修改限制主机：

语法：

hostlimit set <name> { [sa <ip>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] }

参数说明：

name　　设置限制主机的名字

sa　设置限制主机的源 IP 地址，可以是一个 IP 地址或者网段

newconn　　开启限制新建连接的功能

type　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　设置阻断时间，必须大于等于 period

concurrent　　开启限制并发连接的功能

comment　　设置限制主机的注释，可选参数，默认为空

示例：

firewall>hostlimit set webcnct sa 192.168.10.0/255.255.255.0 newconn on type each 100 60 70 concurrent on type share 100 comment “new WEB limition”

3. 显示限制主机：

语法：

hostlimit disp [<name>]

参数说明：

name　　限制主机的名字

示例：

firewall>hostlimit disp webcnct

4. 删除限制主机：

语法：

hostlimit del <name>

参数说明：

name　　　限制主机的名字

示例：

firewall>hostlimit del webcnct

5. 清空限制主机：

语法：

hostlimit clean

示例：

firewall>hostlimit clean

6.14. 限制服务 svclimit

功能：设置限制服务参数。包括：源 IP 地址、目的端口、连接数量、周期、阻断时间等。

1. 添加限制服务：

语法：

svclimit add <name> sa <ip> dp <port> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>]

参数说明：

name　　　设置限制服务的名字

sa　设置限制服务的源 IP 地址，可以是一个 IP 地址或者网段

dp　　设置限制访问的端口号，有效值为 1 至 65535

newconn　　开启限制新建连接的功能

type　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　设置阻断时间，必须大于等于 period

concurrent　　开启限制并发连接的功能

comment　　设置限制服务的注释，可选参数，默认为空

示例：

firewall>svclimit add webcnct sa 192.168.10.1/255.255.255.0 dp 80 newconn on type each 100 60 70 concurrent on type share 100 comment "new service limition"

2. 修改限制服务：

语法：

svclimit set <name> { [sa <ip>] [dp <port>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] }

参数说明：

name　　设置限制服务的名字

sa　设置限制服务的源 IP 地址，可以是一个 IP 地址或者网段

dp　　设置限制访问的端口号，有效值为 1 至 65535

newconn　　开启限制新建连接的功能

type　　设置独占模式或者共享模式

connect　　设置在一个周期内可以接受的连接数量，有效值为 1 至 65535

period　　设置周期，有效值为 1 至 3600（秒）

block　　　设置阻断时间，必须大于等于 period

concurrent　开启限制并发连接的功能

comment　　设置限制服务的注释，可选参数，默认为空

示例：

firewall>svclimit set webcnct sa 192.168.10.1/255.255.255.0 dp 80 newconn on type each 100 60 70 concurrent on type share 100 comment “new service limition”

3. 显示限制服务：

语法：

svclimit disp [<name>]

参数说明：

name　　　限制服务的名字

示例：

firewall>svclimit disp webcnct

4. 删除限制服务：

语法：

svclimit del <name>

参数说明：

name　　　限制服务的名字

示例：

firewall>svclimit del webcnct

5. 清空限制服务：

语法：

svclimit clean

示例：

```
firewall>svclimit clean
```

6.15. 带宽策略 bandwidth

功能：设置带宽策略列表。包括：限制带宽、保证带宽和优先级等。

语法：

```
bandwidth add <name> priority <number> minbw <number> maxbw <number> [ comment <comment> ]
bandwidth set <name> { [ priority <number> ] [ minbw <number> ] [ maxbw <number> ] [ comment <comment> ] }
bandwidth del <name>
bandwidth disp [<name>]
```

参数说明：

name	设置带宽定义的名字
priority	设置带宽定义的优先级，有效值为 0（高优先级）至 3（低优先级）
minbw	设置带宽定义的保证带宽，有效值为 50 至 102400（kbps）
maxbw	设置带宽定义的最大带宽，有效值为 50 至 102400（kbps）
comment	设置带宽定义的注释，可选参数，默认为空

最大带宽必须大于保证带宽（差距应大于 15kbps）；保证带宽之和不能大于接口带宽；

示例：

```
firewall>bandwidth add bw1 priority 0 minbw 1000 maxbw 7000 comment “bandwidth 1”
```

firewall>bandwidth set bw1 priority 2 minbw 100 maxbw 200 comment “new bandwidth 1”

firewall>bandwidth disp

firewall>bandwidth disp bw1

firewall>bandwidth del bw1

6.16. URL 列表 defurl

功能：设置 URL 过滤规则。包括：过滤策略（黑白名单）、过滤端口、过滤的关键字、是否做相关日志记录等。

语法：

defurl add <name> type { blacklist | whitelist } port <port>+ log { none | permit | deny | all } [comment <comment>]

defurl set <name> { [type { blacklist | whitelist }] [port <port>+] [log { none | permit | deny | all }] [comment <comment>]

defurl addkey <name> <keyword>+　　向 URL 过滤规则添加关键字

defurl delkey <name> <keyword>+　　从 URL 过滤规则中删除关键字

defurl del <name>

defurl disp [<name>]

参数说明：

name　　设置 URL 过滤规则的名字

type　　设置 URL 过滤规则的类型，blacklist 表示与关键字匹配以后阻断，whitelist 表示仅允许与关键字匹配以后才能通过

port　　设置一个或多个 URL 过滤规则的端口

log　　设置 URL 过滤规则的日志，none 为不记录日志，permit 为记录允

许访问的 URL，deny 为记录禁止访问的 URL，all 为记录所有 URL

comment 设置 URL 过滤规则的注释，可选参数，默认为空

keyword 关键字，可添加多个

示例：

firewall>defurl add huangse1 type blacklist port 80 8080 log all comment “URL filter 1”

firewall>defurl set huangse1 type whitelist port 88 8888 log none comment “new URL filter 1”

firewall>defurl addkey huangse1 “sex” “xxx” “huangse”

firewall>defurl delkey huangse1 “huangse”

firewall>defurl disp

firewall>defurl disp huangse1

firewall>defurl del huangse1

6.17. 病毒过滤

功能：对所有流经防火墙的流量做病毒检测，阻止被病毒入侵内部网络。

语法：

defantivirus [update { on | off}]

defantivirus set smtp [discard { on | off}] [alarm { on | off }]

defantivirus set smtpfile filenum <number> filesize <number> dirnum <number>

defantivirus import <filename>

defantivirus [disp { state | smtp }]

参数说明：

update 设置是否自动更新病毒库，默认为不自动更新

discard 设置是否丢弃感染病毒的文件，默认为丢弃

alarm	设置是否向发送端报警，默认为向发送端报警
filenum	设置允许传输的最大文件数目
filesize	设置文件最大容量，单位 Mb
dirnum	设置文件压缩的层数限制
import	设置将被导入的病毒库文件名
disp	显示相关设置，state 为显示病毒库的相关设置，smtp 为显示 smtp 的相关设置

示例：

```
defantivirus set smtp discard on alarm on
defantivirus set smtpfile filenum 800 filesize 20 dirnum 5
defantivirus disp state
```

7. 安全策略

本章描述与安全相关的配置命令，包括：安全规则、地址绑定、IDS 产品联动、抗攻击。

7.1. 安全规则 policy

功能：设置安全规则。大部分控制选项推荐使用对象定义中已定义的内容。

1. 添加“允许”安全规则：

语法：

policy add permit [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] [p2p {on | off}]

参数说明：

name　设置安全规则的名字，可选参数，默认为空

id　设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from　设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

to　设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

in 设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out 设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

service 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any”

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

bandwidth 设置带宽控制，可以使用带宽定义、“none”，可选参数，默认为不使用带宽控制

url 设置 URL 过滤，可以使用 URL 过滤规则、“none”，可选参数，默认为不使用 URL 过滤

auth 设置用户认证，可选参数，默认为不使用用户认证

log 设置日志记录，可选参数，默认为不记录日志

hostprotect 设置保护主机，可选参数，默认为不启用保护主机功能

svcprotect 设置保护服务，可选参数，默认为不启用保护服务功能

hostlimit 设置限制主机。可选参数，默认为不启用限制主机功能

svclimit 设置限制服务，可选参数，默认为不启用限制服务功能

tunnel 是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active 设置是否生效，可选参数，默认为生效

p2p 设置 P2P 限制，可选参数，默认为不启用 P2P 限制功能

示例：

firewall>policy add permit name “policy permit 1” id 1 from trust to dmz service http time none bandwidth none url none auth off log off hostprotect off tunnel none active on p2p off

提示：添加示例中的规则之前，必须先定义服务 http(请查阅 defsvc 命令)。

2. 添加“禁止”安全规则：

语法：

policy add deny [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] [p2p {on | off}]

参数说明：

name 设置安全规则的名字，可选参数，默认为空

id 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

to 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

in 设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out 设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

service 设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any”

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

bandwidth 设置带宽控制，可以使用带宽定义、“none”，可选参数，默认为不使用带宽控制

url 设置 URL 过滤，可以使用 URL 过滤规则、“none”，可选参数，默认为不使用 URL 过滤

auth 设置用户认证，可选参数，默认为不使用用户认证

log 设置日志记录，可选参数，默认为不记录日志

hostprotect 设置保护主机，可选参数，默认为不启用保护主机功能

svcprotect 设置保护服务，可选参数，默认为不启用保护服务功能

hostlimit 设置限制主机。可选参数，默认为不启用限制主机功能

svclimit 设置限制服务，可选参数，默认为不启用限制服务功能

tunnel 是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active 设置是否生效，可选参数，默认为生效

p2p 设置 P2P 限制，可选参数，默认为不启用 P2P 限制功能

示例：

firewall>policy add deny name “policy deny 1” id 2 from dmz to trust service http

提示：添加示例中的规则之前，必须先定义地址组 dmz，trust 和服务 http（请查看 defaddr 命令和 defsvc 命令）。

3. 添加“代理”安全规则：

语法：

policy add proxy [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] service <name> proxy <name> [time { <name> | none }] [auth { on | off }] [log { on | off }] [tunnel <name> | none] [active { on | off }]

参数说明：

name 设置安全规则的名字，可选参数，默认为空

id 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

to 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

in 设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out 设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

service 设置服务，可以使用服务、服务组

proxy 设置代理服务类型，可以使用预定义代理服务、用户自定义代理服务

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

auth 设置用户认证，可选参数，默认为不使用用户认证

log 设置日志记录，可选参数，默认为不记录日志

tunnel 是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active 设置是否生效，可选参数，默认为生效

注意 当安全规则的类型为代理时，服务的目的端口必须是单个端口；当代理服务类型为用户自定义代理服务时，目的地址必须为单个 IP 地址。

示例：

firewall>policy add proxy “proxy1” id 3 service http1 proxy http active on

提示：添加示例中的代理规则之前，必须先定义服务 **http1** 和代理 **http**（请查阅 **defsvc** 和 **defproxy** 命令。

4. 添加“NAT”安全规则：

语法：

policy add nat [id <id>] [name <name>] [from { any | <name> | <ip> }] sat { <name> | <ip> | by_route } [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }]

[bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] [p2p {on | off}]

参数说明：

name　设置安全规则的名字，可选参数，默认为空

id　设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from　设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

sat　设置源地址转换，可以使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）、地址池定义，也可以使用 by_route，动态获取防火墙网卡的地址，一般用于防火墙网卡地址通过 adsl 拨号或者 DHCP 获取的地址的情况。

to　设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

in　设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out　设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

service　设置服务，可以使用服务、服务组、“any”，可选参数，默认为“any”

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

bandwidth　设置带宽控制，可以使用带宽定义、“none”，可选参数，默认为不使用带宽控制

url　设置 URL 过滤，可以使用 URL 过滤规则、“none”，可选参数，默认为不使用 URL 过滤

auth 设置用户认证，可选参数，默认为不使用用户认证

log　设置日志记录，可选参数，默认为不记录日志

hostprotect 设置保护主机，可选参数，默认为不启用保护主机功能

svcprotect 设置保护服务，可选参数，默认为不启用保护服务功能

hostlimit 设置限制主机。可选参数，默认为不启用限制主机功能

svclimit 设置限制服务，可选参数，默认为不启用限制服务功能

tunnel 是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active 设置是否生效，可选参数，默认为生效

p2p 设置 P2P 限制，可选参数，默认为不启用 P2P 限制功能

示例：

firewall>policy add nat “nat1” id 4 from any sat 192.168.10.100 to a1 p2p on

提示：添加示例中的 NAT 规则之前，必须先定义地址 a1(请查看 defaddrgrp 命令)。

5. 添加“端口映射”安全规则：

语法：

policy add portmap [id <id>] [name <name>] [from { any | <name> | <ip> }] [sat { <name> | <ip> | none }] pa <ip> ia { <name> | <ip> } [in { any | <interface> }] [out { any | <interface> }] ps <name> is <name> [time { <name> | none }] [bandwidth { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }]

参数说明：

name 设置安全规则的名字，可选参数，默认为空

id 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

sat 设置源地址转换，可以使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP

地址)、地址池定义、“none”，可选参数，默认为不转换

pa　设置公开地址，仅能使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）

ia　设置内部地址，可以使用单个 IP 地址、服务器地址定义

in　设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out　设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

ps　设置对外服务，可以使用服务，不能使用服务组

is　设置内部服务，可以使用服务，不能使用服务组

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

bandwidth　设置带宽控制，可以使用带宽定义、“none”，可选参数，默认为不使用带宽控制

auth 设置用户认证，可选参数，默认为不使用用户认证

log　设置日志记录，可选参数，默认为不记录日志

hostprotect　设置保护主机，可选参数，默认为不启用保护主机功能

svcprotect　设置保护服务，可选参数，默认为不启用保护服务功能

hostlimit 设置限制主机。可选参数，默认为不启用限制主机功能

svclimit　设置限制服务，可选参数，默认为不启用限制服务功能

tunnel　是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active　设置是否生效，可选参数，默认为生效

注意：对外服务和内部服务必须仅包含类型相同的动态协议、TCP 协议、UDP 协议，且目的端口的数量相同。

示例：

firewall>policy add portmap “portmap1” from any sat 192.168.100.1 pa 192.168.100.1 ia http_server ps http is http

提示：添加示例中的端口应设规则之前，必须先定义服务器地址 http_server 和服务 http（请查阅 defsrvaddr 和 defsvc 命令）。

6. 添加“IP 映射”安全规则：

语法：

policy add ipmap [id <id>] [name <name>] [from { any | <name> | <ip> }] [sat { <name> | <ip> | none }] pa <ip> ia { <name> | <ip> } [in { any | <interface> }] [out { any | <interface> }] [time { <name> | none }] [bandwidth { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }]

参数说明：

name　设置安全规则的名字，可选参数，默认为空

id　设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from　设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

sat　设置源地址转换，可以使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）、地址池、“none”，可选参数，默认为不转换

pa　设置公开地址，仅能使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）

ia　设置内部地址，可以使用单个 IP 地址、服务器地址定义

in　设置流入网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

out　设置流出网口，不能使用网络接口“ha”或“mng”，可选参数，默认为“any”

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不

使用时间控制

bandwidth 设置带宽控制，可以使用带宽定义、“none”，可选参数，默认为不使用带宽控制

auth 设置用户认证，可选参数，默认为不使用用户认证

log 设置日志记录，可选参数，默认为不记录日志

hostprotect 设置保护主机，可选参数，默认为不启用保护主机功能

svcprotect 设置保护服务，可选参数，默认为不启用保护服务功能

hostlimit 设置限制主机。可选参数，默认为不启用限制主机功能

svclimit 设置限制服务，可选参数，默认为不启用限制服务功能

tunnel 是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active 设置是否生效，可选参数，默认为生效

示例：

firewall>policy add ipmap “ipmap1”sat sat1 pa 192.168.100.1 ia http_server

提示：添加示例中的 IP 映射规则之前，必须先定义 NAT 地址池和服务 http_server（请查阅 defaddrpool 和 defsvc 命令）。

7. 添加“病毒过滤”安全规则

语法：

policy add ips [id < id >] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [service < name >] [antivirus < name >] [auth { on | off }] [time { <name> | none }] [log { on | off }] [active { on | off }]

参数说明：

name 设置安全规则的名字，可选参数，默认为空

id 设置安全规则的序号，有效值为 1 至 65535，可选参数，默认为最后

from 设置源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

to 设置目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”，可选参数，默认为“any”

service 设置服务，可以使用服务、服务组、“any”，可选参数

antivirus 设置病毒过滤协议

auth 设置用户认证，默认为不启用用户认证功能

time 设置时间控制，可以使用时间定义、时间组定义、“none”，可选参数，默认为不使用时间控制

log 设置日志记录，默认为不启用日志记录功能

active 设置规则生效，默认为生效

示例：

policy add ips id 13 name f13 from any to any service smtp antivirus smtp auth off time none log on active on

8. 修改安全规则：

语法：

policy set id <id> [{ permit | deny | proxy | nat | portmap | ipmap | ips }] [newid <id>] [name <name>] [from { any | <name> | <ip> }] [sat { <name> | <ip> | none }| by_route] [to { any | <name> | <ip> }] [pa <ip>] [ia { <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [proxy <name>] [antivirus < name >] [ps <name>] [is <name>] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [svclimit on | off] [tunnel <name> | none] [active { on | off }] [p2p { on

| off }]

参数说明：

id 指定欲修改的安全规则的序号

type 修改安全规则的类型

name 修改安全规则的名字

newid 修改安全规则的序号，有效值为 1 至 65535

from 修改源地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”

sat 修改源地址转换，可以使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）、地址池、“none”， 也可以使用 by_route，动态获取防火墙网卡的地址，一般用于防火墙网卡地址通过 adsl 拨号或者 DHCP 获取的地址的情况。

to 修改目的地址，可以使用单个 IP 地址、IP 地址/子网掩码、地址定义、地址组定义、“any”

pa 修改公开地址，仅能使用防火墙 IP 地址（不包括网络接口“ha”和“mng”上的 IP 地址）

ia 修改内部地址，可以使用单个 IP 地址、服务器地址定义

in 修改流入网口，不能使用网络接口“ha”或“mng”

out 修改流出网口，不能使用网络接口“ha”或“mng”

service 修改服务，可以使用服务、服务组

proxy 修改代理服务类型，可以使用预定义代理服务、用户自定义代理服务

antivirus 设置病毒过滤协议

ps 修改对外服务，可以使用服务、服务组

is 修改内部服务，可以使用服务、服务组

time修改时间控制，可以使用时间定义、时间组定义、“none”

bandwidth　修改带宽控制，可以使用带宽定义、“none”

url　修改 URL 过滤，可以使用 URL 过滤规则、“none”

auth修改用户认证

log　修改日志记录

hostprotect　修改保护主机

svcprotect　修改保护服务

hostlimit 修改限制主机

svclimit　修改限制服务

tunnel　是否启用 vpn 隧道，默认为 none，不走 vpn 隧道。

active　修改是否生效

p2p 设置 P2P 限制，可选参数，默认为不启用 P2P 限制功能

注意 修改安全规则的类型时，仅类型为允许和禁止的安全规则可以互相转换；某些参数仅能使用在相应类型的安全规则中；在不同类型的安全规则中，相同的参数可能会有不同的取值要求。

示例：

firewall>policy set id 1 deny time timegroup1

提示：输入示例中的命令之前，必须先定义时间组 timegroup1（请查阅 deftimegrp 命令）。

9. 删除所有安全规则：

policy del all

10. 删除指定序号的安全规则：

policy del id <id>

11. 显示安全规则：

policy disp　　　　　　显示所有安全规则的概要信息

policy disp id <id>显示指定安全规则的详细信息

12. 更新安全规则：

policy refresh

修改对象定义后，使用此命令可以让安全规则使用修改后的对象定义。

7.2. 地址绑定 ipmac

功能：设置 IP/MAC 地址绑定，并可以执行 IP/MAC 地址对探测。如果防火墙某网口配置了“IP/MAC 地址绑定 启用功能”、“IP/MAC 地址绑定的默认策略（允许或禁止）”，当该网口接收数据包时，将根据数据包中的源 IP 地址与源 MAC 地址，检查管理员设置好的 IP/MAC 地址绑定表。如果地址绑定表中查找成功，匹配则允许数据包通过，不匹配则禁止数据包通过。如果查找失败，则按缺省策略（允许或禁止）执行。

1. 探测 IP/MAC 地址对：

语法：

ipmac detect if <name>　　　　指定欲从哪个网络接口进行探测

ipmac detect ip <ip>　　　　　　　指定从探测哪个 IP 地址或者网段。若欲探测 IP 地址段，则必须有某防火墙地址在该网段

示例：

firewall>ipmac detect if fe1

firewall>ipmac detect ip 192.168.1.0

2. 添加 IP/MAC 地址对：

语法：

ipmac add <ip> <mac> [if { <name> | none}] [unique { on | off }]

参数说明：

ip　指定 IP 地址

mac 指定 MAC 地址

if　指定相应的网络接口，可选参数，默认为不指定网络接口

unique　指定是否进行 MAC 地址的唯一性检查，可选参数，默认为不检查

示例：

firewall>ipmac add 192.168.1.1 00:23:45:00:12:34 if none unique off

3. 修改 IP/MAC 地址对：

语法：

ipmac set <ip> { [newip <ip>] [mac <mac>] [if { <name> | none }] [unique { on | off }]

参数说明：

ip　修改 IP 址

mac 修改 MAC 地址

if　修改相应的网络接口，可选参数，默认为不指定网络接口

unique　设置是否进行 MAC 地址的唯一性检查，可选参数，默认为不检查

示例：

firewall>ipmac set 192.168.1.1 00:23:45:00:12:34 if any unique on

4. 删除 IP/MAC 地址对：

ipmac del ip <ip>

5. 显示 IP/MAC 地址对：

ipmac disp

提示：必须开启相应网口的 **IP/MAC** 地址绑定功能（请查看 **sysif** 命令），添加的 **IP/MAC** 地址对才起作用。

7.3. P2P 限制

功能：设置 **P2P** 限制

1. 设置 apple 协议限制

语法：

limitp2p set [apple { permit | deny | limit }]

参数说明：

permit	设置为允许使用不作任何限制
deny	设置为禁止使用
limit	允许使用且进行流量控制

示例：

firewall>limitp2p set apple deny

2. 设置 ares 协议限制

语法：

limitp2p set [ares { permit | deny | limit }]

参数说明：

permit　　　　设置为允许使用不作任何限制

deny　　　　设置为禁止使用

limit　　　　允许使用且进行流量控制

示例：

firewall>limitp2p set ares deny

3. 设置 bt 协议限制

语法：

limitp2p set [bt { permit | deny | limit }]

参数说明：

permit　　　　设置为允许使用不作任何限制

deny　　　　设置为禁止使用

limit　　　　允许使用且进行流量控制

示例：

firewall>limitp2p set bt deny

4. 设置 dc 协议限制

语法：

limitp2p set [dc { permit | deny | limit }]

参数说明：

permit　　　　设置为允许使用不作任何限制

deny　　　　设置为禁止使用

limit　　　　允许使用且进行流量控制

示例：

firewall>limitp2p set dc deny

5. 设置 edonkey 协议限制

语法：

limitp2p set [edonkey { permit | deny | limit }]

参数说明：

permit	设置为允许使用不作任何限制
deny	设置为禁止使用
limit	允许使用且进行流量控制

示例：

firewall>limitp2p set edonkey deny

6. 设置 gnu 协议限制

语法：

limitp2p set [gnu { permit | deny | limit }]

参数说明：

permit	设置为允许使用不作任何限制
deny	设置为禁止使用
limit	允许使用且进行流量控制

示例：

firewall>limitp2p set gnu deny

7. 设置 kazaa 协议限制

语法：

limitp2p set [kazaa { permit | deny | limit }]

参数说明：

permit	设置为允许使用不作任何限制

deny 设置为禁止使用

limit 允许使用且进行流量控制

示例：

firewall>limitp2p set kazaa deny

8．设置 soul 协议限制

语法：

limitp2p set [soul { permit | deny | limit }]

参数说明：

permit 设置为允许使用不作任何限制

deny 设置为禁止使用

limit 允许使用且进行流量控制

示例：

firewall>limitp2p set soul deny

9．设置 winmx 协议限制

语法：

limitp2p set [winmx { permit | deny | limit }]

参数说明：

permit 设置为允许使用不作任何限制

deny 设置为禁止使用

limit 允许使用且进行流量控制

示例：

firewall>limitp2p set winmx deny

10．设置流量控制

语法：

limitp2p set bandwidth <name>

参数说明：

name 带宽列表中的带宽名称

示例：

firewall>limitp2p set bandwidth p2p_band

11．查看 P2P 限制设置

语法：

limitp2p disp

7.4. IDS 产品联动 ids

功能：设置 IDS 产品联动。包括主流 IDS 产品。

1. 设置 SUIP 联动：

语法：

ids suip <ip>+ <portt>

参数说明：

ip 设置 SUIP IDS 的 IP 地址

port 设置 SUIP IDS 的联动端口（UDP）

示例：

需要和两台支持 S（firewall Uniform IDS Platform）入侵检测系统联动，其 IP 地址分别为 192.168.200.1 和 192.168.200.2，服务器端口均为 5000

firewall>ids suip 192.168.200.1 192.168.200.2 5000

2. 导入 SUIP 联动证书：

语法：

ids suipcert <filename> <password>

参数说明：

filename　　SUIP 入侵检测系统证书文件名

password　上面所指证书的管理员口令，必须为 9 个字符

需要先用命令“rcvfile”上传证书文件。证书文件和口令可以从 SUIP 入侵检测系统上得到。

示例：

firewall>ids suipcert suip20050101.dat 123456789

3. 开始与 IDS 系统联动：

ids on { suip | venus | netpower | safemate }

示例：

开始与 suip 系统联动：

firewall>ids on suip

联动系统的相应参数必须已经指定正确。

4. 停止与 IDS 系统联动：

ids off { suip | venus | netpower | safemate }

5. 设置“天阗”联动：

ids venus <ip>+ <port>

6. 设置“天眼”联动：

ids netpower <ip>+ <port>

7. 导入“天眼”联动证书：

语法：

ids netpower cacert <filename> consolecert <filename> consolekey <filename>

参数说明：

cacert 设置 CA 证书文件名

consolecert 设置控制台证书文件名

consolekey 设置控制台密钥文件名

需要先用命令“rcvfile”上传证书文件；所有证书必须和相应的“天眼”系统匹配。

示例：

firewall>ids netpower cacert cacert123.pem onsolecert on_cert123.pem onsolekey on_key123.pem

8. 设置 SafeMate 联动：

ids safemate <port>

9. 导入 SafeMate 联动密钥文件：

语法：

ids safematekeyfile <filename>

参数说明：

keyfile 设置密钥文件名

注意事项：

需要先用命令“rcvfile”上传密钥文件。

示例：

firewall>ids safemate keyfile mysafemate.dat

10. 自动阻断的 IP 地址：

防火墙和 IDS 系统联动，默认地，，将自动阻断所有 IDS 系统检测为具有入侵行为（含误报）的 IP 地址。可通过本命令把误报的 IP 地址挑出来，不进行自动阻断，保持通常。

语法：

ids ignoreip <ip>+

示例：

地址为 192.168.100.1 和 192.168.100.2 的内部主机上运行了某些服务，导致了 IDS 系统误报，不希望防火墙阻断这两个 IP 地址，可进行如下设置：

firewall>ids ignoreip 192.168.100.1 192.168.100.2

语法：

ids set ignoreip none

示例：

不忽略任何 IP 地址，即阻断所有被 IDS 检测为有入侵行为的地址，可进行如下设置：

firewall>ids ignoreip none

11. 显示联动设置：

ids disp

7.5. 抗攻击 anti

功能：设置防火墙系统的抗攻击功能，在相应的网络接口上进行设置。

1. 设置抗攻击：

语法：

anti synflood <interface> { <number> | on | off }　　SYN flood 攻击，0－65535（数据包/秒）

anti icmpflood <interface> { <number> | on | off } ICMP flood 攻击，0－65535（数据包/秒）

anti pingofdeath <interface> { <number> | on | off }　　Ping of Death 攻击，0－65535（字节）

anti udpflood <interface> { <number> | on | off }　　UDP flood 攻击，0－65535（数据包/秒）

anti pingsweep <interface> { <number> | on | off }ping sweep 攻击，1－65535（毫秒），为允许 10 个不同 IP 地址的 ICMP 包的时间间隔

anti tcpportscan <interface> { <number> | on | off }　　TCP 端口扫描，1－65535（毫秒），为允许一个 IP 地址的 10 个不同端口的 TCP 包的时间间隔

anti udpportscan <interface> { <number> | on | off }　　UDP 端口扫描，1－65535（毫秒），为允许一个 IP 地址的 10 个不同端口的 UDP 包的时间间隔

anti loosesourcerouteip <interface> { on | off }　　松散源路由攻击

anti strictsourcerouteip <interface> { on | off }　　严格源路由攻击

anti winnuke <interface> { on | off }　　Win Nuke 攻击

anti smurf <interface> { on | off }　　smurf 攻击

anti securityip <interface> { on | off }　　IP 安全选项攻击

anti recordrouteip <interface> { on | off }　　回放路由攻击

anti streamidip <interface> { on | off }　　IP 流攻击

anti timestampip <interface> { on | off }　　IP 时间戳攻击

anti land <interface> { on | off }　　land 攻击

anti teardrop <interface> { on | off }　　　　　　　　泪滴攻击

参数说明：

interface　　　　指定欲设置的网络接口

on　　　在指定网络接口上对某种攻击行为进行检测

启用以后对性能有不同程度的影响

off　　　在指定网络接口上不检查该类别的攻击

number　设置阈值，对于某些种类的攻击，该阈值为检测依据

示例：

firewall>anti synflood fe1 on

firewall>anti icmpflood fe1 off

firewall>anti synflood fe1 200

firewall>anti icmpflood fe1 1000

firewall>anti pingofdeath fe1 800

firewall>anti udpflood fe1 1000

提示：输入示例中命令之前，必须在相应网络接口上开启抗攻击功能（请查看的 sysif 命令）。

2. 显示所有网络接口的抗攻击设置：

anti disp　　　　　　显示网络接口上的抗攻击选项是否开启

anti disp <interface>　显示网络接口上抗攻击功能的详细信息，对某种攻击是否需要进行检测阈值等。

7.6. 入侵防护 ips

1. 攻击类型设置

语法：

ips [atkresp { onlog | ondrop | off }] [backdoor { onlog | ondrop | off }] [info { onlog | ondrop | off }] [multimedia { onlog | ondrop | off }] [p2p { onlog | ondrop | off }] [porn { onlog | ondrop | off }] [scan { onlog | ondrop | off }] [virus { onlog | ondrop | off }] [webcgi { onlog | ondrop | off }] [webclient { onlog | ondrop | off }] [webcf { onlog | ondrop | off }] [webft { onlog | ondrop | off }] [webiis { onlog | ondrop | off }] [webmisc { onlog | ondrop | off }] [webphp { onlog | ondrop | off }]

ips add

参数说明：

atkresp	设置 atkresp 攻击类型
backdoor	设置 backdoor 攻击类型
info	设置 info 攻击类型
multimedia	设置 multimedia 攻击类型
p2p	设置 p2p 攻击类型
porn	设置 porn 攻击类型
scan	设置 scan 攻击类型
virus	设置 virus 攻击类型
webcgi	设置 webcgi 攻击类型
webclient	设置 webclient 攻击类型
webcf	设置 webcf 攻击类型

webft	设置 webft 攻击类型
webiis	设置 webiis 攻击类型
webmisc	设置 webmisc 攻击类型
webphp	设置 webphp 攻击类型

示例：

ips atkresp ondrop

2. 端口设置

语法：

ips add port < port >+	增加端口
ips del port < port >+	删除端口
ips clear port < port >+	清除端口
ips disp	显示入侵防护的相关设置

示例：

ips disp

8. 高可用性

本章描述了高可用性设置的命令。

8.1. HA 基本配置

功能：同步主控制节点与非主控制节点之间的配置和状态，进行 HA 基本参数配置。

语法：

1. 设置 HA 属性

语法：

syncfg set state { master | backup }if <interface> ifip <ip> masterip <ip>

参数说明：

state：是否设置为主控节点，master 是主控节点，backup 是非主控节点。

if：设置监控网口

ifip: 选择监控网口的 ip

masterip : 添加主控节点的 ip

2. 启动/停止自动同步配置

语法：

syncfg autocfg { on | off }

参数说明：

autocfg：自动同步非主控节点与主控节点之间的配置。

3. 启动手工同步配置

语法：

syncfg mancfg

参数说明：

mancfg：手动同步非主控节点与主控节点之间的配置。

4．启动/停止自动同步状态

语法：

syncfg autostate {on | off }

参数说明：

autostate：自动同步非主控节点与主控节点之间的状态。

5．启动手工同步状态

syncfg manstate

manstate：手动同步非主控节点与主控节点之间的状态。

6．显示 ha 设置

语法：

syncfg disp [status { fw | vrrp | vlan }]

参数说明：

status：显示当前状态

fw：显示其它防火墙信息

vrrp：显示其它防火墙设置的 vrrp 信息

vlan：显示其它防火墙设置的 vlan 信息

注意：只有设置为非主控节点并添加了网络接口和主控节点的 ip 后才能同步配置。

注意：手工同步配置需要重起防火墙

8.2. 路由模式 HA

8.2.1.VRRP 实例 vrrp

功能： 用于在防火墙端口上虚拟 VRRP 的 ip 地址，命令配置 VRRP 的工作状态、绑定接口、VRID 以及绑定 IP 地址。

1. 添加 VRRP 实例：

语法：

vrrp add <name> <interface> <vrid> <ip>+ [comment <comment>]

参数说明：

name：指定实例名称

interface：指定网络接口

vrid：实例的 id 号，1~255，不可重复。

ip：虚拟 IP，可添加 ip 或 ip/mask 形式的 IP，最多可添加 20 个 IP。

comment：备注，0 到 256 个字符

示例：

firewall>vrrp add vrrp1 fe1 100 10.50.10.1 comment “vrrp1”

2. 修改 VRRP 实例：

语法：

vrrp set <name> { [interface <interface>] [vrid <vrid>] [ip <ip>+] [comment <comment>] }

参数说明：

name 要修改的 vrrp 设备名称

interface：指定网络接口

vrid：实例的 id 号，1~255，不可重复。

ip：虚拟 IP，可添加 ip 或 ip/mask 形式的 IP，最多可添加 20 个 IP。

comment：备注，0 到 256 个字符

示例：

firewall>vrrp set vrrp1 fe1 vrid 100 ip 10.50.10.2 comment “vrrp1”

3. 删除 VRRP 实例：

语法：

vrrp del <name>
参数说明：

name　　　　　　vrrp 设备名称

示例：

firewall>vrrp del vrrp1

4. 显示 VRRP 实例：

语法：

vrrp disp [<name>]
参数说明：

name　　　　　　vrrp 设备名称

示例：

firewall>vrrp disp vrrp1

8.2.2.VRRP 关联 vrrpbunch

功能：设置 VRRP 实例之间的关联，在 VRRP 关联中的一个 VRRP 实例失效，则属于这个 VRRP 关联的 VRRP 实例同时失效。

1. 增加 VRRP 关联：

语法：

vrrpbunch add <name> [priority <priority>] [comment <comment>]

参数说明：

<name>：指定关联名称

priotity：优先级，1~255，数字越小优先级越高，默认值为 100，可重复

comment：备注

示例：

firewall>vrrpbunch add vrrpbunch1 priority 100 comment “create vrrpbunch1”

2. 删除 VRRP 关联：

语法：

vrrpbunch del <name>

参数说明：

name　　　　vrrp 关联名称

示例：

firewall>vrrpbunch del vrrpbunch1

3. 将 VRRP 实例添加到 VRRP 关联内：

语法：

vrrpbunch addmbr <name> <vrrpname>+

参数说明：

name　　　　vrrp 关联名称　　长度 1—20

vrrpname　　用 vrrp 命令设置的 vrrp 定义

示例：

firewall>vrrpbunch addmbr vrrpbunch1 vrrp1

4. 从 VRRP 关联内删除 VRRP 实例：

语法：

vrrpbunch delmbr <name> <vrrpname>++

参数说明：

name vrrp 关联名称

vrrpname 用 vrrp 命令设置的 vrrp 定义

示例：

firewall>vrrpbunch delmbr vrrpbunch1 vrrp1

5. 删除 VRRP 关联内的所有 VRRP 实例：

语法：

vrrpbunch delallmbr <name>

参数说明：

name vrrp 关联名称

示例：

firewall>vrrpbunch delallmbr vrrpbunch1

6. 查看 VRRP 关联：

语法：

vrrpbunch disp [<name>]

参数说明：

name vrrp 关联名称

示例：

firewall>vrrpbunch disp vrrpbunch1

7. 启用/停止 VRRP 关联：

语法：

vrrpbunch { start <name>+ | stop }

参数说明：

start　　　　启动 **vrrp** 关联

stop　　　　停止 **vrrp** 关联

name　　　　vrrp 关联名称，每次可以启动一个或者多个关联。

示例：

firewall>vrrpbunch start vrrpbunch1

说明：启动 vrrp 关联前，一定要在安全规则的最前面加一条允许到目的地址为 224.0.0.0/255.0.0.0 通过的包过滤规则：

firewall>policy add permit name “vrrppermit 1” id 1 from any to 224.0.0.0/255.0.0.0 service any time none

注意：一个实例可以同属多个关联，但包含同一实例的关联只能启动一个。

8.3. 桥模式 HA

8.3.1.桥配置

1. 设置 pvst 属性

功能：

设置 pvst 的属性

语法：

pvst set <vlanid> priority <number>

参数说明：

<vlanid>：指定设置 vlan 的 id，范围是 2~4096。

priority：设置优先级，范围是 4096~61440，且必须为 4096 的整数倍

2. 开启/关闭 pvst

功能：

启动和停止 pvst

语法：

pvst { on | off }

3. 显示 pvst 设置

功能：

显示 pvst 的相关配置。

语法：

pvst disp [state]

参数说明：

state：是可选参数，如果不带参数，显示 vlanid 和优先级的信息，如果输入参数 state，则显示 pvst 的状态是否启动。

示例：

```
firewall> pvst disp
Vlanid          Priority
firewall> pvst disp state
pvst is off
```

4. 设置 stp 属性

功能：

设置 stp 的属性

语法：

stp set priority <number>

参数说明：

priority：设置优先级，范围是 4096~61440，且必须为 4096 的整数倍

5. 开启/关闭 stp

功能：

启动和关闭 stp 功能

语法：

stp { on | off }

6. 显示 stp 设置

功能：

显示 stp 的相关配置

语法：

stp disp

9. 用户认证

9.1. 用户认证服务器 authsrv

功能：设置用户认证服务器

1. 本地认证服务器：

语法：

authsrv local < port > <port >

参数说明：

port 设置防火墙上的用户认证端口（TCP）

port 设置防火墙上的用户监控端口（UDP）

示例：

使用本地认证服务器，在防火墙上的认证端口为 9998/TCP，在防火墙上的监控端口为 9998/UDP，可进行如下设置：

firewall>authsrv local 9998 9998

2. RADIUS 服务器：

语法：

authsrv radius <ip> < port > < port > <key>

参数说明：

ip 设置 RADIUS 用户认证服务器的 IP 地址

port 设置 RADIUS 用户认证服务器的认证端口（UDP）

port 设置 RADIUS 用户认证服务器的审计端口（UDP）

key　　　　　　设置与防火墙通信时的共享密钥，密钥长度为 6 至 15 个字符

示例：

firewall>authsrv radius 192.168.100.1 1812 1813 abcdefg

3. 启用本地用户认证服务器：

authsrv on local

4. 启用 RADIUS 服务器：

authsrv on radius

5. 显示用户认证服务器：

authsrv disp

9.2. 用户 defuser

功能：设置用户列表。先定义用户组，再定义用户。如果用户属性和组属性发生冲突，以用户属性为准。如果一个用户同时属于多个组，组之间的属性不同或者有冲突，取其最优值（大的、启用的等等），不能累加。

语法：

添加用户：

defuser add <name> password <password> [active { on | off }] [comment <comment>]

修改用户基本信息：

defuser set <name> { [password <password>] [active { on | off }] [comment <comment>] }

把用户加入到用户组：

defuser addgrp <name> < name>+

把用户从用户组中删除：

defuser delgrp <name> < name>+

给用户添加安全规则：

defuser addpolicy <name> { [sa { any | <name> }] [time {none | <name> }] }

删除用户的安全规则：

defuser delpolicy <name> { [sa { any | <name> }] [time {none | <name> }] }

删除用户：

defuser del <name>

显示用户

defuser disp [<name> | online]

显示在线用户信息：

defuser disp online

阻断在线用户：

defuser block { ip <ip> | all }

参数说明：

name	设置用户的名字
password	设置用户的密码，6 至 15 个字符
active	设置用户是否生效，可选参数，默认为生效
comment	设置用户的注释，可选参数，默认为空
name	用户所属的组
sa	设置源地址，可以使用地址定义、地址组定义、“any”，可选参数，默认为空
deftime	设置时间控制，可以使用时间定义、时间组定义，可选参数，默认为空

示例：

firewall>defuser add u1 password 123456 active on comment “Defuser 1”

firewall>defuser set u1 password 12345678 active off comment “new Defuser 1”

把用户 u1 加入到组 ug1、ug2 和 ug3 中：

firewall>defuser addgrp u1 ug1 ug2 ug3

把用户 u1 从组 ug2 和 ug3 中删除，即用户不再隶属于 ug2 和 ug3 组：

firewall>defuser delgrp u1 ug2 ug3

给用户 u1 添加一条安全规则，允许其在 t1 时间段在 a1 地址进行身份验证，从而享受相应的服务：

firewall>defuser addpolicy u1 sa a1 time t1

删除用户 u1 的一条安全规则：

firewall>defuser delpolicy u1 sa a1 time t1

删除用户 u1：

firewall>defuser del name u1

阻断来自 IP 地址 192.168.100.1 的用户：

firewall>defuser block ip 192.168.100.1

阻断所有在线用户：

firewall>defuser block all

提示：输入示例中的命令之前，必须先定义用户组 ug1，ug2，ug3 和时间对象 t1（请查阅 defusergrp 和 deftime 命令）。

9.3. 用户组 defusergrp

功能：设置用户组。必须是已定义的用户。先定义用户组，再定义用户。如果用户属性和组属性发生冲突，以用户属性为准。如果一个用户同时属于多个组，组之间的属

性不同或者有冲突，取其最优值（大的，启用的，等等），不能累加。

1. 用户组：

语法：

defusergrp add <name> [auth { pap | skey }] [traffic { <number> | none }] [time { <number> | none }] [acctexpire { <date> | none }] [pwexpire { <number> | none }] [active { on | off }] [reset { weekly <number> | monthly <number> | none }] [comment <comment>]

defusergrp set <name> { [auth { pap | skey }] [traffic { <number> | none }] [time { <number> | none }] [acctexpire { <date> | none }] [pwexpire { <number> | none }] [active { on | off }] [reset { weekly <number> | monthly <number> | none }] [comment <comment>] }

defusergrp del <name>

defusergrp disp [<name>]

defusergrp disp <name> member

参数说明：

name 设置用户组的名字

auth 设置认证方式，可选参数，默认为 PAP

traffic 设置流量限额，1 至 4194304（KBytes），可选参数，默认为不限制

time 设置时间限额，1 至 65535（分钟），可选参数，默认为不限制

acctexpire 设置帐号失效日期，可选参数，默认为不失效

pwexpire 设置密码过期天数，1 至 999（天），默认为不过期

active 设置用户是否生效，可选参数，默认为生效

reset 设置限额重置周期，可选参数，默认为不重置

comment 设置用户的注释，可选参数，默认为空

示例：

firewall>defusergrp add usergroup1 auth pap traffic 100000 deftime 600 acctexpire 2010/01/01 pwexpire 30 reset weekly 1 comment “user group 1”

firewall>defusergrp set usergroup1 auth skey traffic none deftime none acctexpire none pwexpire none reset none comment “new user group 1”

要显示用户组 usergroup1 的所有成员，可使用如下命令：

firewall>defusergrp disp usergroup1 member

2. 用户组成员：

语法：

defusergrp addmbr < name> <name>+

defusergrp delmbr < name> <name>+

defusergrp delallmbr < name>

参数说明：

name　　指定用户组名

name　　指定欲添加到用户组中的用户名

示例：

firewall>defusergrp addmbr usergroup1 u1 u2 u3

firewall>defusergrp delmbr usergroup1 u1

firewall>defusergrp delallmbr usergroup1

提示：输入示例中的命令之前，必须先定义用户u1，u2，u3（请查阅 67 页的 defuser命令）。

3. 用户组策略：

语法：

defusergrp addpolicy <name> { [sa { any | <name> }] [time { none | name }] }

defusergrp delpolicy <name> { [sa { any | <name> }] [time { none | name }] }

defusergrp delallpolicy <name>

参数说明：

name　　　指定欲添加策略的用户组的名字

sa　　　设置源地址，可以使用地址定义、地址组定义、"any"，可选参数，默认为空

time 设置时间控制，可以使用时间定义、时间组定义，可选参数，默认为空

示例：

用户组 usergroup1 中的用户可以在 t1 时间段内从 a1 地址进行身份认证，可使用以下命令：

firewall>defusergrp addpolicy usergroup1 sa a1 time t1

要删除刚才添加的那条规则，可使用以下命令：

firewall>defusergrp delpolicy usergroup1 sa a1 time t1

提示：输入示例中的命令之前，必须先定义 NAT 地址池 a1 和时间对象 t1（请查阅 defaddrpool 和 deftime 命令）。

4. 用户组服务：

语法：

defusergrp addsvc <name> { [da { any | <name> }] [service { any | <name> }] [time {none | name}] }

defusergrp delsvc <name> { [da { any | <name> }] [service { any | <name> }] [time {none | name]] }

defusergrp delallsvc <name>

参数说明：

name　　　指定欲添加服务的用户组的名字

da　　　设置目的地址，可以使用地址定义、地址组定义、"any"，可选参

	数，默认为空
service	设置服务，可以使用服务定义、服务组定义、“any”，可选参数，默认为空
time	设置时间控制，可以使用时间定义、时间组定义，可选参数，默认为空

示例：

用户组 usergroup1 的成员在通过身份认证以后，可以在 t1 时间段内享受 da1 提供的 s1 服务，可以使用以下命令：

firewall>defusergrp addsvc usergroup1 da da1 service s1 time t1

要删除以上添加的服务，可使用以下命令：

firewall>defusergrp delsvc usergroup1 da da1 service s1 time t1

提示：输入示例中的命令之前，必须先定义地址组 da1，服务 s1 和时间对象 t1（请查阅 defaddr，defsvc 和 deftime 命令）。

10. 系统监控

本章描述如何监控系统的运行状态，包括：网络监控、系统信息、网络接口状态、资源状态、日志信息、在线用户、ARP 表等。

10.1. 网络监控 netmonitor

功能：监控各种网络环境中，被指定的 IP 地址的流量和连接数。分为内网监控，DMZ 区监控，外网监控，内外网监控。

1. 内网监控：

语法：

netmonitor set inner { <saddr> | any } [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+

参数说明：

saddr	源地址，可选择一定义的地址或地址组名称
any	监控所有内网地址
statistic	监控的统计周期，可以是一天或一周
report time	发送邮件报表的时间，可以选择 0 点至 23 点
alertmail	是否用邮件传送统计报表，开启或关闭报告发送功能，on 是开启，off 是关闭
interface	开启监控的端口列表，端口名用空格隔开

示例：

开启内网监控功能，源地址为 any，统计周期为一周，发送邮件报表时间为 17 点，开启邮件报表，监控端口 FE1 和 FE3，可以使用以下命令：

firewall>netmonitor set inner any statistic oneweek report time 17 alertmail on fe1 fe3

2. DMZ 区监控：

语法：

netmonitor set DMZ { <daddr> } [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+

参数说明：

daddr	目的地址，可选择一定义的地址或地址组名称
statistic	监控的统计周期，可以是一天或一周
report time	发送邮件报表的时间，可以选择 0 点至 23 点
alertmail	是否用邮件传送统计报表
interface	开启监控的端口列表，端口名用空格隔开

示例：

开启 DMZ 区监控功能，目的地址为已定义的“server”，统计周期为一周，发送邮件报表时间为 17 点，开启邮件报表，监控端口 FE1 和 FE3，可以使用以下命令：

firewall>netmonitor set DMZ server statistic oneweek report time 17 alertmail on fe1 fe3

3. 外网监控：

语法：

netmonitor set internet { <saddr> | any } [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+

参数说明：

saddr 源地址，可选择一定义的地址或地址组名称

statistic 监控的统计周期，可以是一天或一周

report time 发送邮件报表的时间，可以选择 0 点至 23 点

alertmail 是否用邮件传送统计报表

interface 开启监控的端口列表，端口名用空格隔开

示例：

开启外网监控功能，源地址为 any，统计周期为一周，发送邮件报表时间为 17 点，开启邮件报表，监控端口 FE1 和 FE3，可以使用以下命令：

firewall>netmonitor set internet any statistic oneweek report time 17 alertmail on fe1 fe3

4. 内外网监控：

语法：

netmonitor set intonet { <saddr> | any } <daddr> [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+

参数说明：

saddr 源地址，可选择一定义的地址或地址组名称

daddr 目的地址，可选择一定义的地址或地址组名称

statistic 监控的统计周期，可以是一天或一周

report time 发送邮件报表的时间，可以选择 0 点至 23 点

alertmail 是否用邮件传送统计报表

interface 开启监控的端口列表，端口名用空格隔开

示例：

开启内外网监控功能，源地址为 any，目的地址为已定义的“server”，统计周期为一周，发送邮件报表时间为 17 点，开启邮件报表，监控端口 FE1 和 FE3，可以使用以下命令：

firewall>netmonitor set intonet any server statistic oneweek report time 17 alertmail on fe1 fe3

5. 查看历史纪录：

语法：

netmonitor see history { inner | DMZ | internet | intonet } type { connect | flow } <number>

参数说明：

history	后面指定监控的网络类型
type	显示结果时，IP 地址排序的方式，连接数或是流量
number	查看第几个历史纪录，如果是前一次的，输入 1，往前第 5 次纪录，输入 5

示例：

查看内网监控结果，往前数第三次的历史纪录，并按照连接数排序，可用以下命令：

firewall>netmonitor see history inner type connect 3

6. 查看实时纪录：

语法：

netmonitor see currently { inner | DMZ | internet | intonet } type { connect | flow }

参数说明：

currently	后面指定监控的网络类型
type	显示结果时，IP 地址排序的方式，连接数或是流量

示例：

查看内网监控结果，并按照连接数排序，可用以下命令：

firewall>netmonitor see currently inner type connect

7. 显示监控设置：

语法：

netmonitor disp [inner | DMZ | internet | intonet]
参数说明：

disp　　　　　　后面指定监控的网络类型

示例：

查看内网的设置，可用以下命令：

firewall>netmonitor disp inner

8. 清空所有监控纪录：

语法：

netmonitor clean { inner | DMZ | internet | intonet }
参数说明：

示例：

清空所有纪录，可用以下命令：

firewall>netmonitor clean inner

9. 关闭网络监控功能：

语法：

netmonitor active { inner | DMZ | internet | intonet } off
参数说明：

active　　　　　　指定监控的网络类型

示例：

关闭 DMZ 区监控功能：

firewall>netmonitor active DMZ off

10.2. 系统信息 sysinfo

功能：显示系统工作状态。此处查看的内容包括：软硬件版本信息、网口状态、CPU 和内存的利用率等。

1. 显示系统基本信息：

语法：

sysinfo disp　　显示系统名称、软硬件版本号、序列号等信息

2. 显示所有网络接口的状态：

语法：

sysinfo disp if　　显示所有网络接口活动状态、收发包数量等

3. 显示指定网络接口的状态：

语法：

sysinfo disp if <interface>　显示指定网络接口当前详细状态

4. 显示 CPU 利用率：

语法：

sysinfo disp cpu

5. 显示内存利用率：

语法：

sysinfo disp memory

10.3. 看日志 log

功能：查看防火墙本地日志信息。

1. 显示所有日志：

语法：

log disp

2. 显示指定类型的日志：

语法：

log disp type { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 }

参数说明：

type 指定欲显示的日志类型

1：安全规则日志

2：代理日志

3：IDS 日志

4：VPN 日志

5：用户认证日志

6：内容过滤日志

7：病毒过滤日志

8：设备状态日志

9：设备管理日志

10：集群日志

11：扩展日志

3. 显示指定优先级的日志：

语法：

log disp priority { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 }

参数说明：

priority	指定欲显示的日志优先级
	0：紧急事件
	1：报警事件
	2：危险事件
	3：错误事件
	4：警告事件
	5：通知事件
	6：消息事件
	7：调试事件

4. 清除日志：

语法：

log clear



清除防火墙上所有的日志。

10.4. ipsec 隧道监控

功能：

显示隧道的状态信息。

语法：

vpn show ph2 tunnel {all | <tunnelname>}

参数说明：

参 数	描 述
<tunnel_name>	要监控隧道的名称

示例：

监控隧道 cl_test：

firewall>vpn show ph2 tunnel cl_test

10.5. 在线用户 defuser

语法：

defuser disp online

10.6. 查看 ARP 表 arp

功能：查看、修改、清除防火墙上的 ARP 表。

1. 显示 ARP 表：

语法：

arp disp

2. 将防火墙上的所有 ARP 转换为静态 ARP：

语法：

arp static

3. 清除防火墙上的 ARP：

语法：

arp clear

10.7. IP 探测 ping

语法：

ping { <ip> | <hostname> }　　根据 IP 地址或根据主机名探测主机

10.8. 域名查询 dnssearch

语法：

dnssearch <ip>　　查询指定 IP 地址的主机名

dnssearch <hostname>　　查询指定主机的 IP 地址

示例：

firewall>dnssearch 192.168.100.1

server1

firewall>dnssearch server1

192.168.1.1

10.9. 路由探测 traceroute

功能：根据 IP 地址或者主机名探测数据包从防火墙到远程主机经过的路由。

语法：

traceroute { <ip> | <hostname> }

示例：

firewall>traceroute 192.168.200.1

traceroute to 192.168.200.1 (192.168.200.1), 30 hops max, 38 byte packets

 1　192.168.1.254 (192.168.1.254)　0.100 ms　0.100 ms　0.100 ms

2　192.168.2.1 (192.168.2.1)　0.100 ms　0.100 ms　0.100 ms

11. 其它

11.1. 接收文件 rcvfile

功能：使用 ZMODEM 协议接收管理主机发送的文件。

语法：

rcvfile



需要管理主机上的终端支持 ZMODEM 协议。

示例：

firewall>rcvfile

11.2. 显示分页 disppage

功能：设置 CLI 的分页显示功能。

语法：

disppage on	开启分页显示功能
disppage off	关闭分页显示功能
disppage	显示当前分页功能是否开启

11.3. 设置提示符 prompt

功能：设置提示字符串。

1. 设置提示字符串：

语法：

prompt <string>

示例：

firewall>prompt　youname

youname>

2. 恢复提示字符串：

语法：

prompt

示例：

youname>prompt firewall

firewall>

11.4. 退出命令行界面 quit

语法：

quit

12. 使用技巧

命令行界面提供以下功能键：

？键	获得上下文相关的帮助信息
TAB 键	自动补全命令，若有多个选择，则打印出可选项
上下箭头	翻滚以前提交过的命令，可存储最近的 100 条命令
CTRL+C	中止正在执行的命令
回车键	提交命令

在命令行界面还提供丰富的编辑命令，其功能键如下：

←	光标前移一格
→	光标后移一格
CTRL+A	光标移到行首
CTRL+E	光标移到行尾
CTRL+D	删除光标处的单个字符
CTRL+H	删除光标前的单个字符
CTRL+U	清空当前命令行
CTRL+C	忽略当前命令行，在下一行显示新的命令提示符

13. 命令索引

命 令	语 法	页数
adsl（ADSL 拔号）	adsl set [type { manual | bootup | schedule time <name> }] [interface <name>] [username <name>] [password <password>] [dyndomain { on domain <domainname> domainuser <name> domianpasswd <password> | off }] [autodial { on | off }] [active { on | off }] adsl { connect | disconnect } adsl disp [status]	41
anti（抗攻击）	anti synflood <interface> { <number> | on | off } anti icmpflood <interface> { <number> | on | off } anti pingofdeath <interface> { <number> | on | off } anti udpflood <interface> { <number> | on | off } anti pingsweep <interface> { <number> | on | off } anti tcpportscan <interface> { <number> | on | off } anti udpportscan <interface> { <number> | on | off } anti loosesourcerouteip <interface> { on | off } anti strictsourcerouteip <interface> { on | off } anti winnuke <interface> { on | off } anti smurf <interface> { on | off } anti securityip <interface> { on | off }	137

	anti recordrouteip <interface> { on | off } anti streamidip <interface> { on | off } anti timestampip <interface> { on | off } anti land <interface> { on | off } anti teardrop <interface> { on | off } anti disp [<name>]	
arp （ARP 表）	arp static arp clear arp disp	167
authsrv （用户认证服务器）	authsrv local <port> <port> authsrv radius <ip> <port> <port> <key> authsrv on { local | radius } authsrv disp	151
bandwidth （带宽定义）	bandwidth add <name> priority <number> minbw <number> maxbw <number> [comment <comment>] bandwidth set <name> { [priority <number>] [minbw <number>] [maxbw <number>] [comment <comment>] } bandwidth del <name> bandwidth disp [<name>]	111
defaddr （地址定义）	defaddr add <name> <ip> [<comment>] defaddr set <name> { [ip <ip>] [comment <comment>] } defaddr del <name> defaddr disp [<name>]	82
defaddrgrp	defaddrgrp add <name> [<comment>]	83

（地址组）	defaddrgrp set <name> <comment> defaddrgrp addmbr <name> <name>+ defaddrgrp delmbr <name> <name>+ defaddrgrp del <name> defaddrgrp disp [<name>]	
defaddrpool（NAT 地址池）	defaddrpool add <name> <ip> [comment <comment>] defaddrpool set <name> { [ip <ip>] [comment <comment>] } defaddrpool del <name> defaddrpool disp [<name>]	85
defmail（邮件过滤）	defmail set smtp sender [<keyword>+] defmail { on | off } smtp sender defmail set smtp receiver [<keyword>+] defmail { on | off } smtp receiver defmail set smtp subject [<keyword>+] defmail { on | off } smtp subject defmail set smtp content [<keyword>+] defmail { on | off } smtp content defmail set smtp attach [<keyword>+] defmail { on | off } smtp attach defmail set pop3 sender [<keyword>+] defmail { on | off } pop3 sender defmail set pop3 receiver [<keyword>+] defmail { on | off } pop3 receiver defmail set pop3 subject [<keyword>+] defmail { on | off } pop3 subject	95

	defmail set pop3 attach [<keyword>+] defmail { on | off } pop3 attach defmail disp {smtp | pop3}	
defproxy （代理服务）	defproxy set http { [port <port>] [java { permit | deny }] [javascript { permit | deny }] [activex { permit | deny }] } defproxy set ftp { [port <port>] [get { permit | deny }] [put { permit | deny }] [multi { permit | deny }] } defproxy set telnet port <port> defproxy set smtp { [port <port>] [domain <domainname>+] [server <domainname>] [maildomain <domainname>+] [mailserver <ip>+] [maxlength <number>] [maxreceiver <number>] [sendinterval <number>] [sendamount <number>] } defproxy set pop3 { [port <port>] [maxlength <number>] } defproxy set socks port <port> defproxy add custom <name> port <port> [comment <comment>] defproxy set custom <name> { [port <port>] [comment <comment>] } defproxy del custom <name> defproxy disp { default | custom }	92
defsrvaddr （服务器地址）	defsrvaddr add <name> ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight	84

	<number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>]]]]]]]] [comment <comment>] defsrvaddr set <name> { [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>] [ip <ip> [weight <number>]]]]]]]]] [comment <comment>] } defsrvaddr del <name> defsrvaddr disp [<name>]	
defsvc （服务定义）	defsvc add <name> ftp <port> [comment <comment>] defsvc add <name> h323 <port> [comment <comment>] defsvc add <name> sqlnet <port> [comment <comment>] defsvc add <name> icmp [type { 0 | 3 [code { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 }] | 4 | 5 [code { 0 | 1 | 2 | 3 }] | 8 | 9 | 10 | 11 [code { 0 | 1 }] | 12 [code { 0 | 1 }] | 13 | 14 | 17 | 18 }] [comment <comment>] defsvc add <name> proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> |	87

	<number> } [proto{ { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> }]]]]]]] [comment <comment>] defsvc set <name> ftp <port> defsvc set <name> h323 <port> defsvc set <name> sqlnet <port> defsvc set <name> icmp [type { 0 | 3 [code { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 9 | 10 | 11 | 12 | 13 | 14 | 15 }] | 4 | 5 [code { 0 | 1 | 2 | 3 }] | 8 | 9 | 10 | 11 [code { 0 | 1 }] | 12 [code { 0 | 1 }] | 13 | 14 | 17 | 18 }] defsvc set <name> proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto{ { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> } [proto { { tcp | udp } <port> <port> | <number> }]]]]]]] defsvc set <name> comment <comment> defsvc del <name> defsvc disp { dynamic | icmp | common | <name> }	
defsvcgrp （服务组）	defsvcgrp add <name> [comment <comment>] defsvcgrp set <name> comment <comment> defsvcgrp addmbr<name> <name>+	90

	defsvcgrp delmbr<name> <name>+ defsvcgrp delallmbr <name> defsvcgrp del <name> defsvcgrp disp [<name>]	
deftime （时间定义）	deftime add <name> once <date> <time> <date> <time> [comment <comment>] deftime add <name> week { [sun <time>] [mon <time>] [tue <time>] [wed <time>] [thu <time>] [fri <time>] [sat <time>] } [comment <comment>] deftime set <name> once { [<date> <time> <date> <time>] [comment <comment>] } deftime set <name> week { [sun <time>] [mon <time>] [tue <time>] [wed <time>] [thu <time>] [fri <time>] [sat <time>] [comment <comment>] } deftime del <name> deftime disp [<name>]	97
deftimegrp （时间组）	deftimegrp add <name> [comment <comment>] deftimegrp set <name> comment <comment> deftimegrp addmbr <name> <name>+ deftimegrp delmbr <name> <name>+ deftimegrp delallmbr <name> deftimegrp del <name> deftimegrp disp [<name>]	99
defurl （URL 过滤规则）	defurl add <name> type { blacklist | whitelist } port <port>+ log { none | permit | deny | all } [comment <comment>]	112

	defurl set <name> { [type { blacklist | whitelist }] [port <port>+] [log { none | permit | deny | all }] [comment <comment>] defurl addkey <name> <keyword>+ defurl delkey <name> <keyword>+ defurl del <name> defurl disp [<name>]	
defuser （用户定义）	defuser add <name> password <password> [active { on | off }] [comment <comment>] defuser set <name> { [password <password>] [active { on | off }] [comment <comment>] } defuser addgrp <name> <name>+ defuser delgrp <name> <name>+ defuser addpolicy <name> { [sa { any | <name> }] [time {none |<name> }] } defuser delpolicy <name> { [sa { any | <name> }] [time {none |<name> }] } defuser del <name> defuser disp [<name> | online] defuser block { ip <ip> | all }	152
defusergrp （用户组）	defusergrp add <name> [auth { pap | skey }] [traffic { <number> | none }] [time { <number> | none }] [acctexpire { <date> | none }] [pwexpire { <number> | none }] [active { on | off }] [reset { weekly <number> | monthly <number> | none }] [comment <comment>] defusergrp set <name> { [auth { pap | skey }] [traffic	154

	{ <number> | none }] [time { <number> | none }] [acctexpire { <date> | none }] [pwexpire { <number> | none }] [active { on | off }] [reset { weekly <number> | monthly <number> | none }] [comment <comment>] } defusergrp addmbr <name> <name>+ defusergrp delmbr <name> <name>+ defusergrp delallmbr <name> defusergrp addpolicy <name> { [sa { any | <name> }] [time <name> | none] } defusergrp delpolicy <name> { [sa { any | <name> }] [time <name> | none] } defusergrp delallpolicy <name> defusergrp addsvc <name> { [da { any | <name> }] [service { any | <name> }] [time <name> | none] } defusergrp delsvc <name> { [da { any | <name> }] [service { any | <name> }] [time <name> | none] } defusergrp delallservice <name> defusergrp del <name> defusergrp disp [<name>] defusergrp disp <name> member	
dhcp (主机动态配置)	dhcpserver add domain vpnclient { off <network> <netmask> | on <vpnmask> } <range> [gateway <gateway>] [dns <dns>] [domainname <domainname>] [comment <comment> dhcpserver add static <hostname> <mac> <ip> [<comment>]	43

	dhcpserver del domain id <id> dhcpserver del static id <id> dhcpserver start dhcpserver stop dhcpserver disp { domain | static | leases | state} dhcpclient <interface> on dhcpclient disp [status] dhcprelay set server <ip> if <name> dhcprelay { start | stop } dhcprelay disp	
disppage（显示分页）	disppage [on | off]	170
dns（域名服务器）	dns set ip <ip> [<ip>] dns set sysname <name> dns clear dns disp	22
dnssearch（域名服务器查询）	dnssearch { <ip> | <hostname> }	168
fastsetup（配置向导）	fastsetup	32
hostlimit（限制主	hostlimit add <name> sa <ip> { [newconn { on { type { each| share} <connect> <period> <block> } | off }]	106



机）	[concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>] hostlimit set <name> { [sa <ip>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] } hostlimit del <name> hostlimit disp [<name>] hostlimit clean	
hostprotect （保护主机）	hostprotect add <name> sa <ip> da <ip> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>] hostprotect set <name> { [sa <ip>] [da <ip>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] } hostprotect del <name> hostprotect disp [<name>] hostprotect clean	100
ids （IDS 联动）	ids suip <ip>+ <port> ids suipcert <filename> <password> ids venus <ip>+ <port> ids netpower <ip>+ <port> ids netpower cacert <filename> consolecert <filename>	130

	consolekey <filename> ids safemate <port> ids safematekeyfile <filename> ids ignoreip { <ip>+ | none } ids on { suip | venus | netpower | safemate } ids off { suip | venus | netpower | safemate } ids disp	
log （日志）	log disp log disp type { 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 } log disp priority { 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 } log clear	165
logsrv （日志服务器）	logsrv set <ip> <port> udp logsrv clear logsrv disp	21
ipmac （MAC 地址绑定）	ipmac detect if <name> ipmac detect ip <ip> ipmac add <ip> <mac> [if { <name> | none }] [unique { on | off }] ipmac set <ip> { [newip <ip>] [mac <mac>] [if { <name> | none }] [unique { on | off }] } ipmac del <ip> ipmac disp	128
mngacct （管理员帐号）	mngacct add <name> <password> [manager { on | off }] [policyer { on | off }] [auditor { on | off }] mngacct set <name> { [password <password>] [manager { on | off }] [policyer { on | off }] [auditor	25

	{ on | off }] } mngacct del <name> mngacct multi { on | off } mngacct disp	
mngcert （管理证书）	mngcert add cacert <filename> syscert <filename> syskey <filename> mngcert add <filename> mngcert del <filename> mngcert on <filename> mngcert off <filename> mngcert disp { cacert | syscert | admincert }	27
mngglobal （集中管理）	mngglobal add snmpip <ip> [<ip> ...] mngglobal set [snmpip <ip>] [principal <string>] [telephone <string>] [cpu <percent>] [mem <percent>] [fs <percent>] [rcomm <string>] [wcomm <string>] [trapc <string>] [status <string>] [comment <string>] mngglobal unset [snmpip] [principal] [telephone] [cpu] [mem] [fs] [rcomm] [wcomm] [trapc] [status] [comment] mngglobal del snmpip <ip> [<ip> ...] mngglobal on mngglobal off mngglobal disp mngglobal beepalarm on|off	29
mnghost （管理主机）	mnghost add <ip> [<comment>] mnghost del <ip> mnghost disp	24

mngmailbox（报警邮箱）	mngmailbox set <email> [smtp <ip> port <port>] mngmailbox clear mngmailbox disp	20
mngmode（管理方式）	mngmode ssh { on | off } mngmode disp	23
mngpass（管理员口令）	mngpass	27
netmonitor（网络监控）	netmonitor set inner { <saddr> | any } [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+ netmonitor set DMZ <daddr> [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+ netmonitor set internet { <saddr> | any } [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+ netmonitor set intonet { <saddr> | any } <daddr> [[statistic { oneday | oneweek }] [report time <number>] [alertmail { on | off }] [comment <comment>]] <interface>+ netmonitor see history { inner | DMZ | internet | intonet }	159

	type { connect | flow } <number> netmonitor see currently { inner | DMZ | internet | intonet } type { connect | flow } netmonitor disp [inner | DMZ | internet | intonet] netmonitor clean { inner | DMZ | internet | intonet } netmonitor active { inner | DMZ | internet | intonet } off	
ping （主机探测）	ping { <ip> | <hostname> }	168
policy （安全规则）	policy add permit [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] policy add deny [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active	115

	{ on | off }] policy add proxy [id <id>] [name <name>] [from { any | <name> | <ip> }] [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] service <name> proxy <name> [time { <name> | none }] [auth { on | off }] [log { on | off }] [tunnel <name> | none] [active { on | off }] policy add nat [id <id>] [name <name>] [from { any | <name> | <ip> }] sat { <name> | <ip> | by_route } [to { any | <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] policy add portmap [id <id>] [name <name>] [from { any | <name> | <ip> }] [sat { <name> | <ip> | none }] pa <ip> ia { <name> | <ip> } [in { any | <interface> }] [out { any | <interface> }] ps <name> is <name> [time { <name> | none }] [bandwidth { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] policy add ipmap [id <id>] [name <name>] [from	

	{ any | <name> | <ip> }] [sat { <name> | <ip> | none }] pa <ip> ia { <name> | <ip> } [in { any | <interface> }] [out { any | <interface> }] [time { <name> | none }] [bandwidth { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [tunnel <name> | none] [active { on | off }] policy set id <id> [{ permit | deny | proxy | nat | portmap | ipmap }] [newid <id>] [name <name>] [from { any | <name> | <ip> }] [sat { <name> | <ip> | none }| by_route] [to { any | <name> | <ip> }] [pa <ip>] [ia { <name> | <ip> }] [in { any | <interface> }] [out { any | <interface> }] [service { any | <name> }] [proxy <name>] [ps <name>] [is <name>] [time { <name> | none }] [bandwidth { <name> | none }] [url { <name> | none }] [auth { on | off }] [log { on | off }] [hostprotect {on | off }] [svcprotect {on | off }] [hostlimit {on | off }] [svclimit {on | off }] [svclimit on | off] [tunnel <name> | none] [active { on | off }] policy del all policy del id <id> policy disp policy disp id <id> policy refresh	
PPTP/L2TP （PPTP 和	pptpserver set iprange <name> encrypt { 40 | 56 | 128 } auth { [chap] [chapms] [chapms-v2] } [dns <ip>+]	78

L2TP 协议配置）	[wins <ip>+] pptpuser add <name> <password> [<ip>] [<comment>] pptpuser set <name> { [password <password>] [ip <ip> | none] [comment <comment>] } pptpserve r start pptpserver stop pptpserver disp pptpuser del <name> pptpuser disp [online] [<name>] pptpuser del <name> pptpuser disp [online] [<name>]	
prompt （设置提示符）	prompt [<string>]	170
pvst （桥）	pvst set <vlanid> priority <number> pvst { on | off } pvst disp [state] stp set priority <number> stp { on | off } stp disp	148
quit （退出 CLI）	quit	171
rcvfile （接收文件）	rcvfile	170
route （静态路	route set default <ip> route clear default	38

由）	route add sroute <sip> <dip> <nexthop> route del sroute <sip> <dip> route add droute <dip> <nexthop> route del droute <dip> route add mroute <dip> <nexthop> <weight> <nexthop> <weight> [<nexthop> <weight>] route del mroute <dip> route disp	
runtime（运行时间）	runtime	15
svclimit（限制服务）	svclimit add <name> sa <ip> dp <port> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>] svclimit set <name> { [sa <ip>] [dp <port>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] } svclimit del <name> svclimit disp [<name>] svclimit clean	108
svcprotect（保护服务）	svcprotect add <name> sa <ip> da <ip> dp <port> { [newconn { on { type { each| share} <connect> <period> <block> } | off}] [concurrent { on { type { each | share} <connect> } | off }] } [comment <comment>]	103

	svcprotect set <name> { [sa <ip>] [da <ip>] [dp <port>] [newconn { on { type { each | share } <connect> <period> <block> } | off }] [concurrent { on { type { each | share } <connect> } | off}] [comment <comment>] } svcprotect del <name> svcprotect disp [<name>] svcprotect clean	
syncfg（HA 基本配置）	syncfg set state { master | backup }if <interface> ifip <ip> masterip <ip> syncfg autocfg { on | off } syncfg mancfg syncfg autostate {on | off } syncfg manstate syncfg disp [status { fw | vrrp | vlan }]	142
syscfg（系统配置）	syscfg save syscfg reset syscfg import <filename> syscfg export <filename> [encrypt { on | off }] sz <filename>	142
sysif（网络接口）	if set <interface> {[speed { auto | 100full | 100half | 10full | 10half | 1000full | 1000half } [mtu <number>] [ipmac { on | off }] [macpolicy { permit | deny }] [mode { broute | route }] [sroute { on | off }] [log { on | off }] [vlan { <id>+ | trunk | off }] [anti { on | off }] [nonip { permit | deny }] [idsblock { on | off }] }	34

	sysif set vlanroute { on | off } sysif disp [<interface>]	
sysinfo（系统信息）	sysinfo disp sysinfo disp if [<interface>] sysinfo disp cpu sysinfo disp memory	164
sysip（防火墙 IP 地址）	sysip add <interface> <ip> <netmask> [admin { on | off }] [ping { on | off }] [traceroute { on | off }] sysip del <ip> sysip disp	37
systime（系统时钟）	systime set <date> <time> systime disp	14
sysupdate（模块升级）	sysupdate <filename> sysupdate disp	17
timeout（超时退出时间）	timeout { set <number> } timeout disp	15
timesrv（时钟服务器）	timesrv set <ip> <number> timesrv clear timesrv on timesrv off timesrv sync timesrv disp	16

traceroute （路由探测）	traceroute { <ip> | <hostname> }	168
vpn （虚拟专用网）	vpn set default [prekey <prekey>] [ikelifetime <ikelifetime>] [ipseclifetime <ipseclifetime>] [vpnstatus <on|off>] vpn show default vpn set dhcp active{on|off} dhcpserver <dhcpserverip> interface <interface> vpn show dhcp vpn on vpn off vpn add group name <groupname> idtype <psk|rsasig> [clientid <clientid>] [clientcert <clientcert>] [prekey <prekey>] vpn set group name <groupname> idtype <psk|rsasig> [clientid <clientid>] [clientcert <clientcert>] [prekey <prekey>] vpn del group <groupname> vpn add remote static|dynamic aggr psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localid <localid>] [remoteid <remoteid>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>] vpn add remote static|dynamic aggr psk name	49

	<remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>] vpn add remote static main psk name <remote_name> addr <ip> prekey <prekey> [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>] vpn add remote static|dynamic main psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>] vpn add remote static|dynamic main psk name <remote_name> [vpngroup <groupname>] [addr <ip>] [localcert <localcert>] [remotecert <remotecert>] [ike {{des|3des|aes|aes256}-{md5|sha1}-{dh1|dh2|dh5}}] [nat_t {on|off}] [ikelifetime <ikelifetime>] [dpddelay <dpddelay> dpdtimeout <dpdtimeout>] vpn show remote {all | <remotename>} vpn del remote <remotename> vpn active remote <remotename> vpn inactive remote <remotename>	

	vpn add tunnel name <tunnelname> local <local> remote <remote> [auth {esp|ah|comp}] [ipsec <{3des|aes128|aes256|null}-{md5|sha1}>] [pfs on|off dh_group <1|2|5>] [ipseclifetime <ipseclifetime>] proxy_localip <proxy_localip> proxy_localmask <proxy_localmask> proxy_remoteip <proxy_remoteip> proxy_remotemask < proxy_remotemask> vpn show tunnel {all | <tunnelname>} vpn del tunnel <tunnelname> vpn active tunnel <tunnelname> vpn inactive tunnel <tunnelname> vpndev add <dev_name> <tunnel_name> [<comment>] vpndev del <dev_name> vpndev disp	
vrrp（虚拟路由冗余协议）	vrrp add <name> <interface> <vrid> <ip>+ [comment <comment>] vrrp set <name> { [interface <interface>] [vrid <vrid>] [ip <ip>+] [comment <comment>] } vrrp del <name> vrrp disp [<name>]	144
vrrpbunch（vrrp 关联）	vrrpbunch add <name> [priority <priority>] [comment <comment>] vrrpbunch del <name> vrrpbunch addmbr <name> <vrrpname>+ vrrpbunch delmbr <name> <vrrpname>++	145

	vrrpbunch delallmbr <name> vrrpbunch disp [<name>] vrrpbunch { start <name>+ | stop }	